MANUAL

Versão: 10/06/14

AKER Configuration Manager

AKER

www.aker.com.br

1 Indice

1 Indice 2

2 Indice de Figuras 3

3 Introdução 9

3.1 Como está disposto este manual. 9

3.2 Apresentação do Produto 9

3.3 Interface Remota 10

4 Instalando o Aker Configuration Manager 13

4.1 Instalando a Interface Remota (Windows) 13

4.2 Instalação em plataforma Linux 18

5 Utilizando a Interface Remota 21

5.1 O que é a administração remota do Aker Configuration Manager? 21

5.2 Como funciona a administração remota do Aker Configuration Manager? 21

5.3 Iniciando a interface remota 22

5.4 Finalizando a administração remota 36

5.5 Ativação de Licença 37

5.6 Ativando a licença do Firewall pelo Aker Configuration Manager 40

5.7 Renovação da licença 44

5.8 Efetuando as mudanças (commit) 44

5.9 Controlando as Mudanças 45

6 Administrando Usuários do Aker Configuration Manager 51

6.1 Utilizando a Interface Remota 51

7 Configuração de parâmetros 64

7.1 Configurando os Parâmetros 64

8 Cadastrando Entidades 70

8.1 Cadastrando entidades utilizando a Interface Remota 71

9 O Filtro de Estados....76

9.1 Editando uma lista de regras usando a Interface Remota....77

9.2 Associações....80

9.3 Exceções de validação de integridade....84

10 Visualizando o log do Sistema....89

10.1 Configuração de log....90

10.2 Visualização de log....92

11 Monitoramento....98

11.1 Aker Dashboard....99

12 Gerenciando Firewalls....103

12.1 Configurando Firewalls no Aker Configuration Manager....105

12.2 Atualizando Objetos do Firewall....107

12.3 Verificando Status....108

13 Apêndice A - Copyrights e Disclaimers....113

2 Indice de Figuras

Figura 1 – Escolha de idioma para a instalação....14

Figura 2 – Janela de apresentação do instalador do Aker Configuration Manager....14

Figura 3 – Contrato de Licença....15

Figura 4 – Personalizando sua instalação....16

Figura 5 – Iniciando a instalação....16

Figura 6 – Barra de status da instalação....17

Figura 7 – Aker Configuration Manager foi instalado com sucesso....17

Figura 8 – Script de instalação em plataforma Linux Server....18

Figura 9 – Aker Configuration Manager foi instalado com sucesso....19

Figura 10 – Janela de acesso: Aker Configuration Manager....22

Figura 11 – Opções da Interface Remota 23
Figura 12 – Tempo de sessão ociosa 23
Figura 13 - Opção para a exibição das regras 24
Figura 14 – Desabilitar perguntas da Interface Remota 24
Figura 15 – Opções de idiomas da Interface Remota 24
Figura 16 – Alterando a cor de fundo da Interface Remota 25
Figura 17 – Mensagem ao sair da Interface Remota 25
Figura 18 - Menu Janelas 25
Figura 19 – Dispositivos remotos da Interface remota (Control Center) 26
Figura 20 – Janela de Entidades 26
Figura 21 – Menu Ajuda da Interface Remota 27
Figura 22 – Opções de configuração de atualização automática 27
Figura 23 – Notificador de Atualizações 27
Figura 24 – Notificador de Instalação de Atualizações 28
Figura 25 – Atualizações prontas 28
Figura 26 – Informações sobre a Aker Control Center 29
Figura 27 – Menu de Opções do dispositivo remoto 30
Figura 28 – Informação sobre a Entidade 31
Figura 29 – Tipo de Autenticação (Usuário e senha) 32
Figura 30 - Tipo de Autenticação (X.509) 33
Figura 31 – Ícone: Carregar certificado 34
Figura 32 – Ícone: Informações do certificado 34
Figura 33 - Tipo de Autenticação (Agente externo) 35
Figura 34 – Finalizando a administração remota 36
Figura 35 – Botão: Sair 36
Figura 36 – Ativação de Licença 38
Figura 37 – Janela para carregar os dados da licença 39

Figura 38 – Ativando a Licença....40
Figura 39 - Objetos gerenciáveis (Status) 41
Figura 40 – Janela Status....41
Figura 41 – Janela de ativação de licença 42
Figura 42 – Janela de localização do arquivo da licença....43
Figura 43 – Janela de ativação da licença 43
Figura 44 – A licença foi aplicada com sucesso....44
Figura 45 – janela de acesso: Efetuar mudanças 45
Figura 46 – Auditoria: Controle de mudanças 45
Figura 47 – Janela de controle de mudanças....46
Figura 48 – Opções da Janela de controle de mudanças....46
Figura 49 – Janela de Histórico de mudanças....47
Figura 50 – Janela de Publicação 48
Figura 51 – Opções de publicação 49
Figura 52 – Configurações: Gerenciamento de usuários....51
Figura 53 – Aba Usuários internos....52
Figura 54 – Aba X.509....56
Figura 55 – Aba Agentes externos 59
Figura 56 – Aba Fazer busca nos autenticadores....61
Figura 57 – Configurações: Parâmetros....65
Figura 58 – Aba Parâmetros globais 65
Figura 59 – Aba Controle de Acesso 67
Figura 60 – Aba Pooling....68
Figura 61 – Aba genéricas 71
Figura 62 – Aba Grupos....72
Figura 63 – Incluindo /editando máquinas 73
Figura 64 – Políticas: Regras de filtragem....77

Figura 65 – Janela de Regras de filtragem 77
Figura 66 – Opções da Janela de regras de filtragem 79
Figura 67 – Políticas: Associações 80
Figura 68 – Aba Editar 81
Figura 69 – Menu de opções 82
Figura 70 – Adicionando Firewalls 82
Figura 71 – Adicionando ou removendo Políticas 83
Figura 72 – Associações: Aba Editar 83
Figura 73 – Associações: Aba Visualizar 84
Figura 74 – Exceções de validação de integridade 84
Figura 75 - Janela de configurações 85
Figura 76 - Menu Status 86
Figura 77 - Janela Status 86
Figura 78 - Menu de opções da Janela Status 87
Figura 79 - Ícones de opção 87
Figura 80 - Log: Configuração de log 90
Figura 81 - Configurações Gerais 90
Figura 82 - Ações das Mensagens 91
Figura 83 – Log: Visualização de log 92
Figura 84 – Barra de ferramentas de Log 92
Figura 85 – Ícone: Abre a janela do Aker Configuration Manager 93
Figura 86 – Ícone: Para a busca atual 93
Figura 87 – Ícone: Exportar resultados 93
Figura 88 – Ícone: Limpar log 93
Figura 89 – Ícone: Habilita a atualização do log de acordo com o tempo especificado 93
Figura 90 – Ícone: Tempo para atualização das informações de log 93
Figura 91 – Ícone: Mostrar resultados recentes e antigos 93

Figura 92 – Ícone: Expandir mensagens de log 94
Figura 93 – Janela Filtro de eventos 94
Figura 94 – Janela Log 95
Figura 95 - Monitoramento 98
Figura 96 – Janela Alertas 98
Figura 97 – Janela do Dashboard 99
Figura 98 – Editando servidor no Aker Dashboard 100
Figura 99 – Aker Dashboard 101
Figura 100 – Usuários administradores 104
Figura 101 – Usuários Internos 104
Figura 102 – Configurando um novo dispositivo remoto 105
Figura 103 – Editando um novo dispositivo remoto 106
Figura 104 – Atualizando objetos do Firewall 107
Figura 105 – Janela Atualização dos objetos 107
Figura 106 – Objetos gerenciáveis: Status 108
Figura 107 – Janela Status 109
Figura 108 – Menu de opções da Janela de Status 110
Figura 109 – Barra de ferramentas de Status 111

Introdução

3 Introdução

Seja bem-vindo ao manual do usuário do Aker Configuration Manager

Nos próximos capítulos você aprenderá como configurar esta ferramenta de gerenciamento de vários Firewalls simultaneamente. Esta introdução tem como objetivo descrever a organização deste manual e tentar tornar sua leitura o mais simples e agradável possível.

3.1 Como está disposto este manual.

Este manual está organizado em vários capítulos. Cada capítulo mostrará um aspecto da configuração do produto e todas as informações relevantes ao aspecto tratado.

Todos os capítulos começam com uma introdução teórica sobre o tema a ser tratado seguido dos aspectos específicos de configuração do Aker Configuration Manager. Juntamente com esta introdução teórica, alguns módulos possuem exemplos práticos do uso do serviço a ser configurado, em situações hipotéticas, porém bastante próximas da realidade. Buscamos com isso tornar o entendimento das diversas variáveis de configuração o mais simples possível.

Recomendamos que este manual seja lido pelo menos uma vez por inteiro, na ordem apresentada. Posteriormente, se for necessário, pode-se usá-lo como fonte de referência (para facilitar seu uso como referência, os capítulos estão divididos em tópicos, com acesso imediato pelo índice principal. Desta forma, pode-se achar facilmente a informação desejada).

Em vários locais deste manual, aparecerá o símbolo ( ) seguido de uma frase escrita em letras vermelhas. Isto significa que a frase em questão é uma observação muito importante e deve ser totalmente entendida antes de prosseguir com a leitura do capítulo.

3.2 Apresentação do Produto

Produtividade, eficiência e eficácia são conceitos que toda empresa busca para o seu sucesso. Mesmo com todo o avanço da tecnologia, ainda se fazem necessárias novas ideias para tornar mais eficaz o dia a dia dessas empresas. Um bom exemplo disso são os Firewalls que vieram para facilitar e tornar mais protegida a rede de uma empresa, segura dos malfeitores que navegam na grande rede.

Neste contexto, nota-se que o uso de Firewalls é indispensável numa rede de computadores e que a manutenção de vários deles funcionando simultaneamente, pode causar transtornos indesejáveis.

Pensando nisso, a Aker Security Solutions desenvolveu uma ferramenta incrível capaz de gerenciar vários Firewalls ao mesmo tempo. O Aker Configuration Manager, uma ferramenta que permite aplicar em uma única Interface Remota, regras de filtragem e gerenciar diversos Firewalls espalhados por vários locais do mundo. Note que não há a necessidade de instalá-lo nas máquinas que terão Firewall.

Esta versão é compatível com o Aker Firewall, e cada Firewall pode ser acessado e configurado individualmente pelo Aker Configuration Manager, e as informações de configuração são salvas em uma cópia local na máquina. Se outra pessoa acessar o Firewall diretamente (ou seja, sem usar o Configuration Manager) e modificar sua configuração, na próxima vez que o Configuration Manager for utilizado, as modificações feitas diretamente serão perdidas. A cópia local feita pelo Aker Configuration Manager sempre prevalecerá.

3.3 Interface Remota

A Interface Remota é de uso bastante intuitivo e está disponível para plataformas Windows 2000 ou superiores, Fedora Core 8 ou superiores.

O Aker Configuration Manager

Permite gerenciar vários Firewalls ao mesmo tempo. Ele foi criado para ser compatível com o Aker Firewall e atualmente permite aplicar em massa as regras de filtragem.

Copyrights do Sistema

Copyright (c) 1997-2006 Aker Security Solutions.

Utiliza a biblioteca SSL escrita por Eric Young (cay@mincon.oz.au). Copyright © 1995 Eric Young.

Utiliza o algoritmo AES implementação do Dr. B. R. Gladman (brg@gladman.uk.net).

Utiliza o algoritmo MD5 retirado da RFC 1321. Copyright © 1991-2 RSA Data Security, Inc.

Utiliza a biblioteca CMU SNMP. Copyright© 1997 Carnegie Mellon University.

Utiliza a biblioteca de compressão Zlib. Copyright © 1995-1998 Jean-loup Gailly and Mark Adler.

Utiliza a biblioteca QWT escrita por Josef Wilgen. Copyright © 1997.

Inclui software desenvolvido pela Universidade da California, Berkeley e seus colaboradores.

Inclui software desenvolvido por Luigi Rizzo, Universita` di Pisa Portions Copyright 2000 Akamba Corp.

Inclui software desenvolvido por Niklas Hallqvist, Angelos D. Keromytis and Haan Olsson.

Inclui software desenvolvido por Ericsson Radio Systems

Instalando o Aker Configuration Manager

4 Instalando o Aker Configuration Manager

Este capítulo mostra como se instala o Aker Configuration Manager, e quais são seus requisitos.

Requisitos de hardware e software

Para a Interface Remota

A Interface Remota de administração do Aker Configuration Manager roda em plataformas Windows, Linux server (***O Aker Configuration Manager é homologado somente no FEDORA 17 32 bits***), plataformas de 32 bits Intel ou compatíveis.

Para que a Interface Remota execute de maneira satisfatória os componentes de hardware devem possuir as seguintes configurações:

Computador Intel core 2 dual ou superior;

4 Giga bytes de memória RAM;

HD de 500 Giga bytes ou superior;

Placa de rede 10/100 Giga bytes ou superior;

Todos os componentes do hardware devem ser suportados pelo sistema operacional na qual a interface será instalada, em alguma das versões aceitas pelo produto.

4.1 Instalando a Interface Remota (Windows)

A Interface Remota poderá ser instalada nas plataformas Windows ou Linux (***O Aker Configuration Manager é homologado somente no FEDORA 17 32 bits***).

Faça o download e instale ***Aker Control Center plugin for Aker Control Center*** no site:

http://www.aker.com.br/node/1099.

Selecione o idioma no qual deseja realizar a instalação (Português ou Inglês) e clique no botão ***'OK'.***

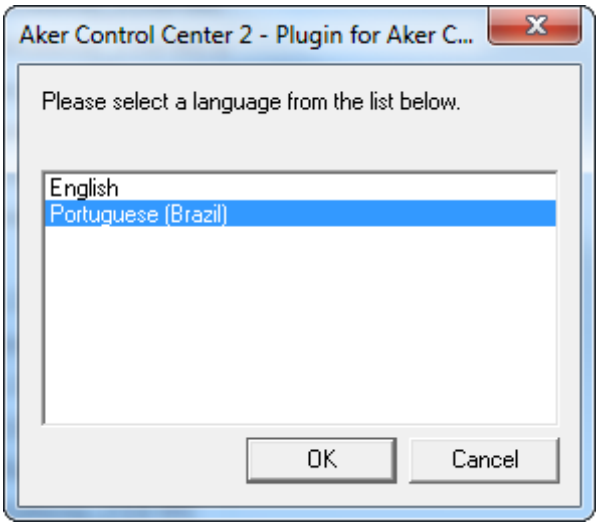

Figura 1 – Escolha de idioma para a instalação

A tela **'Bem-vindo ao Assistente de Instalação'** será exibida. Leia as recomendações e clique no botão **'Avançar'.**

Aker Control Center 2 - Plugin for Aker Configuration M...
AKER CONFIGURATION MANAGER
Bem-vindo ao Assistente de Instalação do Aker Control Center 2 - Plugin for Aker Confi...
Recomendamos que você feche todos programas Windows antes de executar este programa de instalação.
Clique em Cancelar para sair do programa de instalação, em seguida feche quaisquer programas que estiverem sendo executados. Clique em Avançar para continuar a instalação.
AVISO: Este programa está protegido por leis de copyright e tratados internacionais.
A reprodução não autorizada ou distribuição deste programa, ou qualquer parte do mesmo, pode resultar em severas penalidades civis e criminais que serão aplicadas na extensão máxima possível permitida por lei.
AKER
< Voltar
Avançar >
Cancelar

Figura 2 – Janela de apresentação do instalador do Aker Configuration Manager

Em seguida, a tela com o ***'Contrato de Licença do Programa'*** *será exibida*. Leia todas as informações com atenção.

Selecione a opção 'Aceito o contrato de licença' e clique em 'Avançar'.

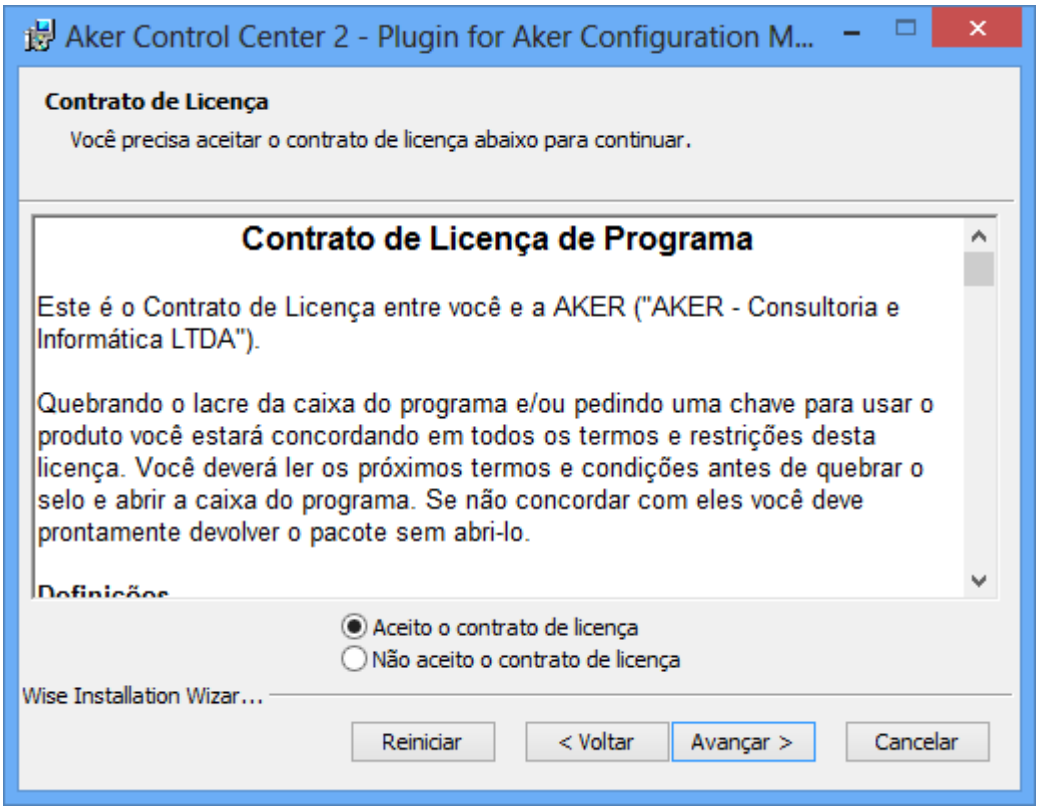
Aker Control Center 2 - Plugin for Aker Configuration M...
Contrato de Licença
Você precisa aceitar o contrato de licença abaixo para continuar.
Contrato de Licença de Programa
Este é o Contrato de Licença entre você e a AKER ("AKER - Consultoria e Informática LTDA").
Quebrando o lacre da caixa do programa e/ou pedindo uma chave para usar o produto você estará concordando em todos os termos e restrições desta licença. Você deverá ler os próximos termos e condições antes de quebrar o selo e abrir a caixa do programa. Se não concordar com eles você deve prontamente devolver o pacote sem abri-lo.
Definições
Aceito o contrato de licença
Não aceito o contrato de licença
Wise Installation Wizar...
Reiniciar
< Voltar
Avançar >
Cancelar

Figura 3 – Contrato de Licença

A seguir, a tela de ***'Informações do usuário'*** será exibida contendo os seguintes campos:

Nome completo: nome do usuário;

Empresa: nome da empresa.

Abaixo aparece um texto, dizendo que as configurações do aplicativo podem ser instaladas para o usuário atual ou para todos os que partilham o computador (para isso é necessário ter direitos de administrador). Escolher uma das opções: ***'Qualquer pessoa que usa este computador'*** ou ***'Somente para mim'***.

Ao término, clique em ***'Avançar'***.

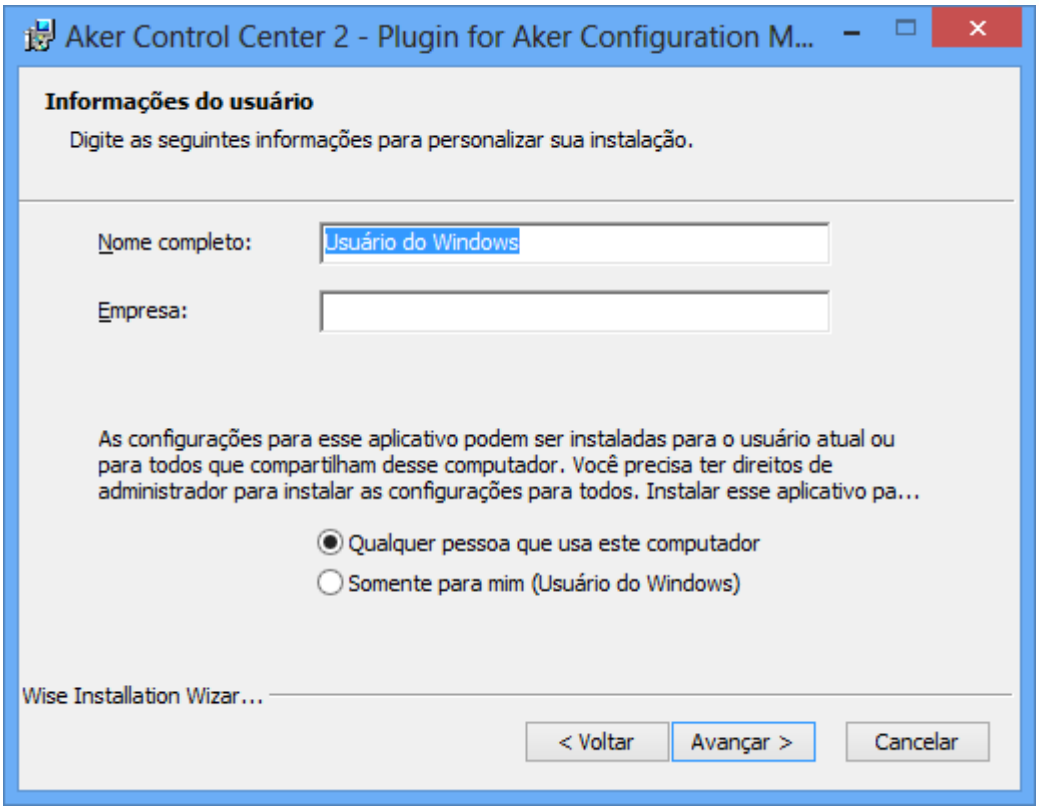
Aker Control Center 2 - Plugin for Aker Configuration M...
Informações do usuário
Digite as seguintes informações para personalizar sua instalação.
Nome completo:
Usuário do Windows
Empresa:
As configurações para esse aplicativo podem ser instaladas para o usuário atual ou para todos que compartilham desse computador. Você precisa ter direitos de administrador para instalar as configurações para todos. Instalar esse aplicativo pa...
Qualquer pessoa que usa este computador
Somente para mim (Usuário do Windows)
Wise Installation Wizar...
< Voltar
Avançar >
Cancelar

Figura 4 – Personalizando sua instalação

A mensagem '*Pronto para instalar o aplicativo*' será exibida. Clique em '*Avançar*'.

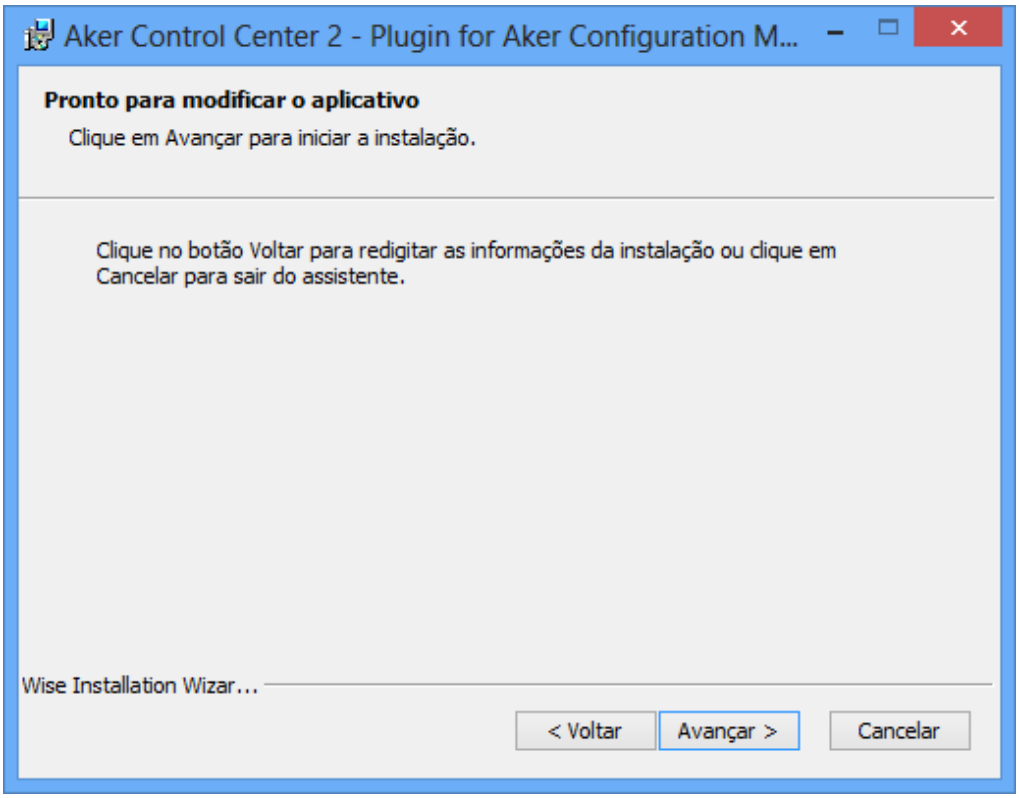
Aker Control Center 2 - Plugin for Aker Configuration M...
Pronto para modificar o aplicativo
Clique em Avançar para iniciar a instalação.
Clique no botão Voltar para redigitar as informações da instalação ou clique em Cancelar para sair do assistente.
Wise Installation Wizar...
< Voltar
Avançar >
Cancelar

Figura 5 – Iniciando a instalação

É possível verificar o status da instalação através da barra de status na tela ***'Atualizando o sistema'***.

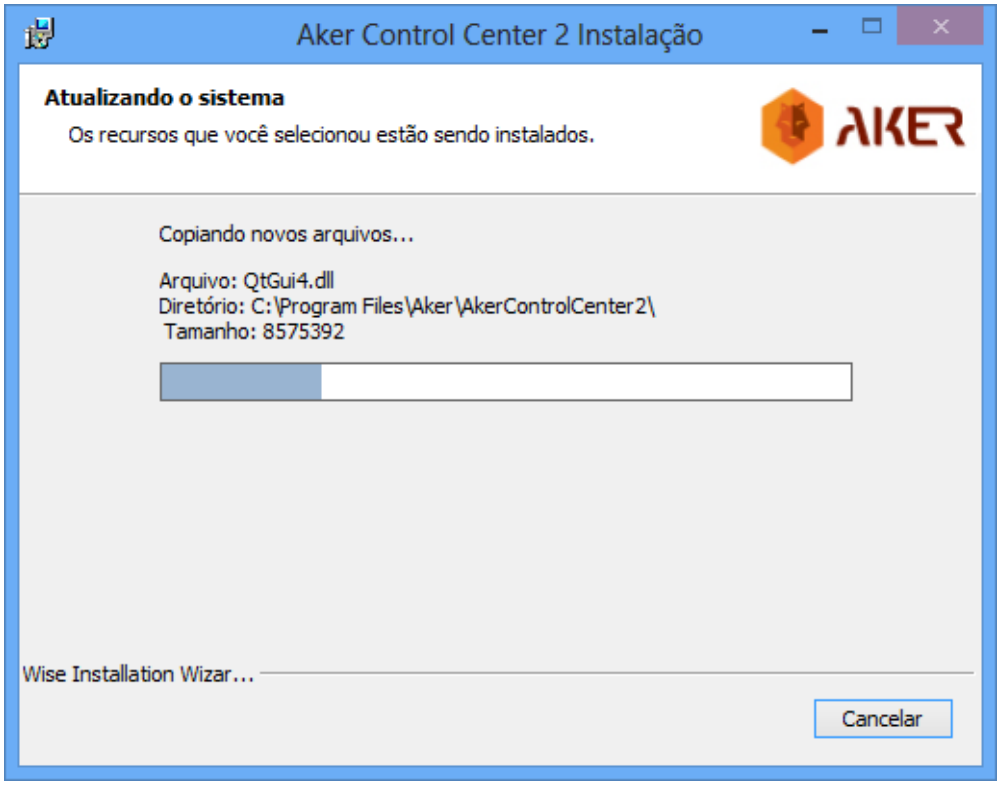

Figura 6 – Barra de status da instalação

Ao concluir a instalação será apresentada a mensagem que o *'Aker Control Center 2 – Plugin for Aker Configuration Manager 2.2* foi instalado com êxito'.

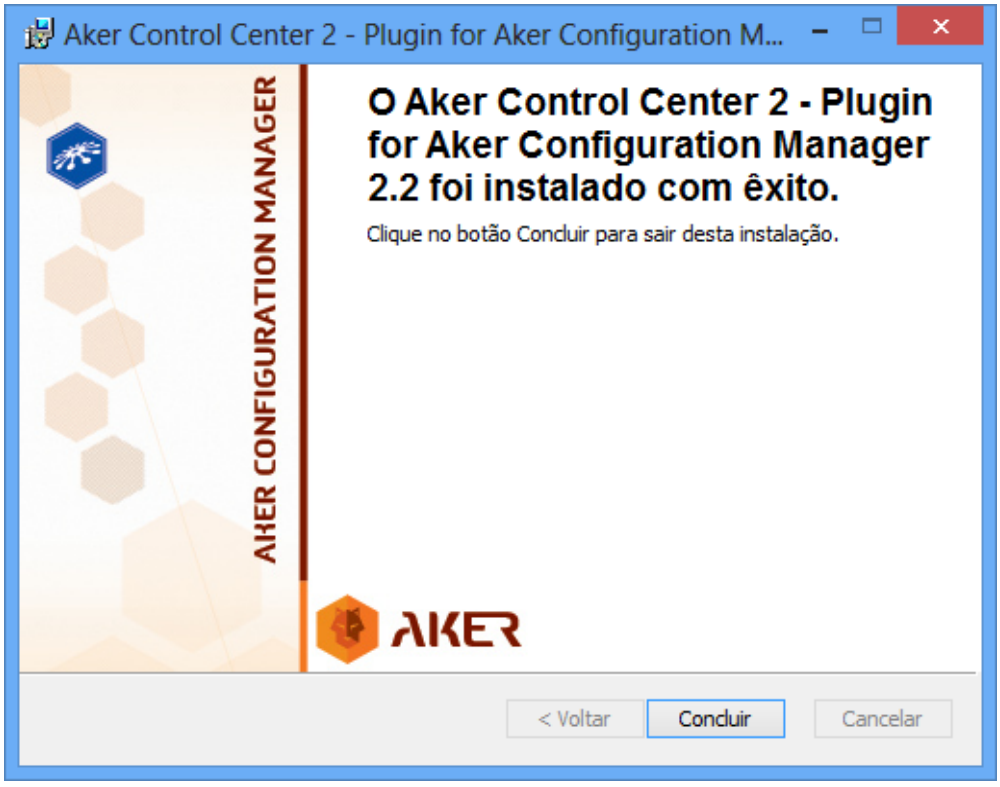
Aker Control Center 2 - Plugin for Aker Configuration M...
AKER CONFIGURATION MANAGER
O Aker Control Center 2 - Plugin for Aker Configuration Manager 2.2 foi instalado com êxito.
Clique no botão Concluir para sair desta instalação.
< Voltar
Concluir
Cancelar

Figura 7 – Aker Configuration Manager foi instalado com sucesso

Para finalizar a instalação, clique em ***'Concluir'.***

4.2 Instalação em plataforma Linux

Para instalar o Aker Configuration Manager em uma plataforma *Linux Server* siga as instruções abaixo (***O Aker Configuration Manager está disponível somente para o Ubuntu server 32 bits 12.04***)

1. Faça o download do Aker Configuration Manager no site: www.aker.com.br.
2. Criar uma pasta e copiar o instalador do Aker Configuration Manager para esta, então inicie a instalação do produto.

Ex: ./ akerconfigurationmanager-2.2-pt-linux-010

3. A janela a seguir será exibida, pressione a tecla "**S**" para prosseguir com a instalação, ou "**N**" para abortar a instalação.

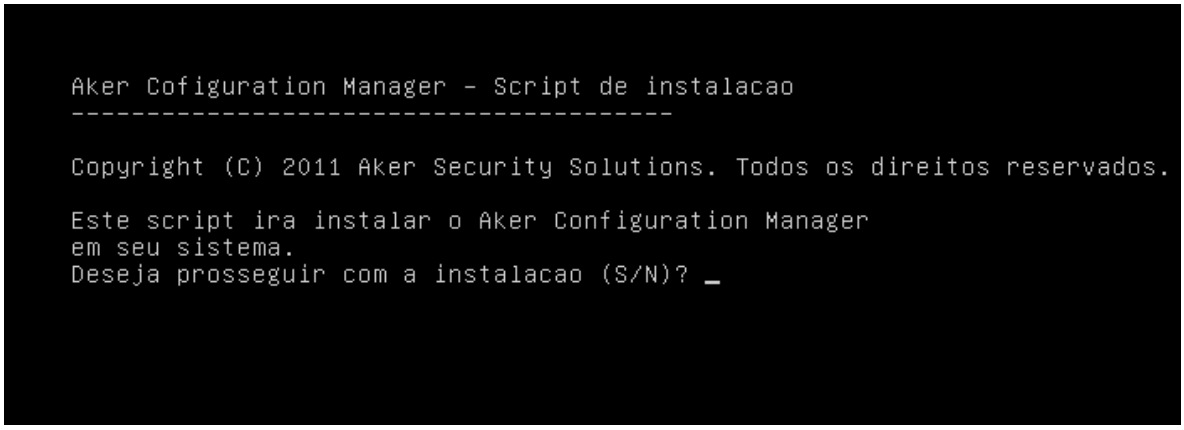
Aker Cofiguration Manager - Script de instalacao
Copyright (C) 2011 Aker Security Solutions. Todos os direitos reservados.
Este script ira instalar o Aker Configuration Manager
em seu sistema.
Deseja prosseguir com a instalacao (S/N)?

Figura 8 – Script de instalação em plataforma Linux Server

4. *Aker Configuration Manager foi instalado com sucesso*, agora se deve cadastrar o nome do usuário administrador, e senha. Após confirmar a senha o usuário administrador estará cadastrado.

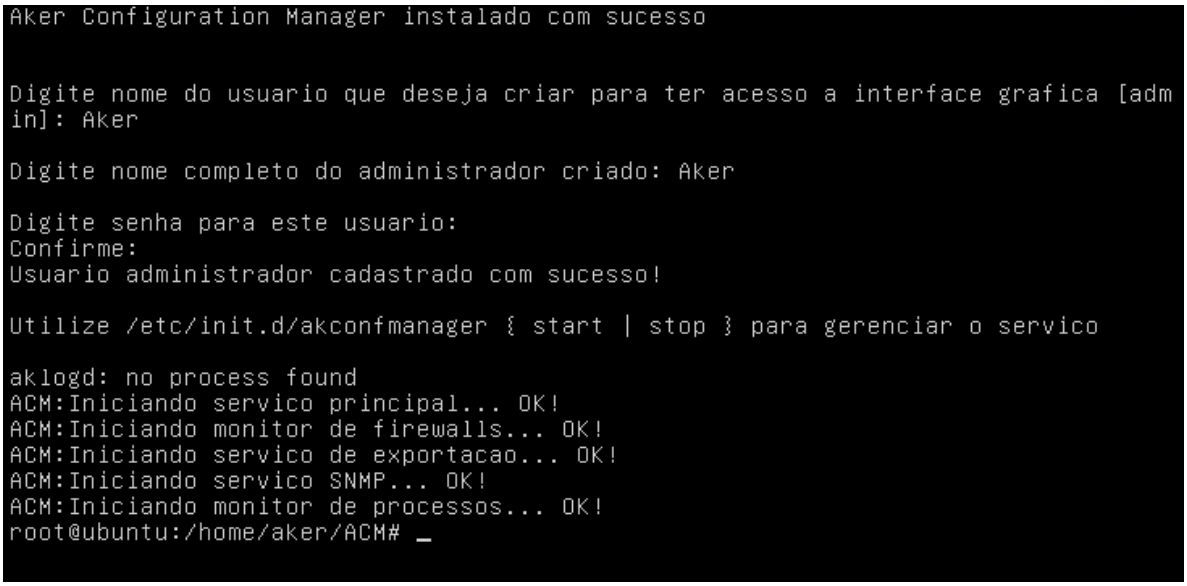
Aker Configuration Manager instalado com sucesso
Digite nome do usuario que deseja criar para ter acesso a interface grafica [adm
in]: Aker
Digite nome completo do administrador criado: Aker
Digite senha para este usuario:
Confirme:
Usuario administrador cadastrado com sucesso!
Utilize /etc/init.d/akconfmanager { start | stop } para gerenciar o servico
aklogd: no process found
ACM:Iniciando servico principal... OK!
ACM:Iniciando monitor de firewalls... OK!
ACM:Iniciando servico de exportacao... OK!
ACM:Iniciando servico SNMP... OK!
ACM:Iniciando monitor de processos... OK!
root@ubuntu:/home/aker/ACM#

Figura 9 – Aker Configuration Manager foi instalado com sucesso

5. Para gerenciar o serviço utilize o comando: /etc/init.d/akconfmanager

Utilizando a Interface Remota

5 Utilizando a Interface Remota

Neste capítulo mostraremos como funciona a Interface Remota de administração do Aker Configuration Manager.

5.1 O *que* é a administração remota do Aker Configuration Manager*?*

O Aker Configuration Manager pode ser totalmente configurado e administrado remotamente a partir de qualquer máquina que possua um sistema operacional compatível com uma das versões da interface remota, que tenha TCP/IP e que consiga acessar a máquina na qual o Configuration Manager se encontra. Isto permite um alto grau de flexibilidade e facilidade de administração, possibilitando que um administrador monitore e configure vários **Aker Configuration Managers** a partir de sua estação de trabalho.

Além dessa facilidade, a administração remota permite uma economia de recursos na medida em que possibilita que a máquina que rode o Aker Configuration Manager não possua monitor e outros periféricos.

5.2 Como funciona a administração remota do Aker Configuration Manager?

Toda a comunicação entre a interface remota e o Aker Configuration Manager é feita de maneira segura, utilizando-se criptografia e autenticação. Para cada sessão são geradas novas chaves de criptografia e autenticação. Além disso, são empregadas técnicas de segurança para impedir outros tipos de ataques como, por exemplo, ataques de repetição de pacotes.

Seguem comentários sobre algumas observações importantes sobre a administração remota:

Só é possível a abertura de uma conexão de administração remota em um determinado instante. Se já existir uma interface conectada, pedidos subsequentes de conexão serão negados e a interface remota informará que já existe uma sessão ativa.

Cada um dos usuários que for utilizar a interface remota deve estar cadastrado no sistema. O programa de instalação pode criar automaticamente um administrador com poderes para cadastrar os demais administradores. Caso se tenha eliminado este administrador ou perdido sua senha, é necessário o uso do módulo local da Interface Remota ou da Interface Texto (via SSH) para criar um novo administrador. Detalhes de como fazer isso se encontram no capítulo intitulado Administrando Usuários do Aker Configuration Manager.

5.3 Iniciando a interface remota

Para iniciar a execução da Interface Remota deve-se executar um dos seguintes passos:

Em máquinas Windows, clique no menu **"Iniciar"** e Selecionar **"Aker Control Center 2"**.

Em Linux deve-se executar o comando ***'/usr/local/aker/control_center2/aker_control_center2_init.sh'*** a partir do prompt do shell ou Clique no ícone criado na área de trabalho (apenas para KDE).

Então a janela abaixo será exibida:

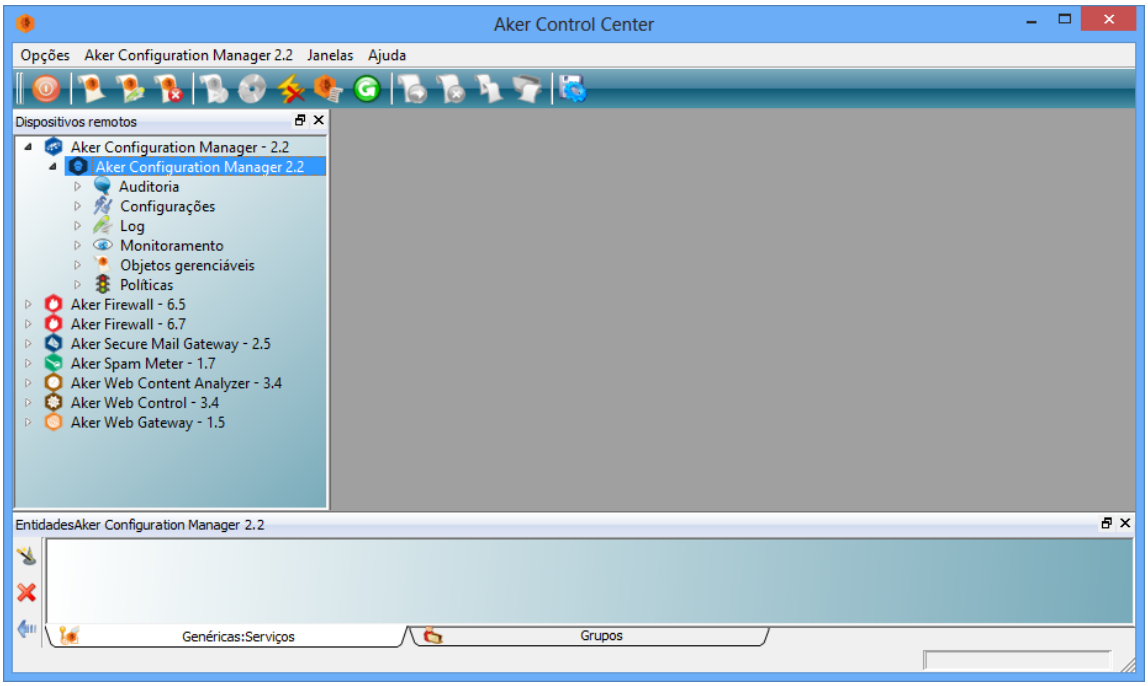

Figura 10 – Janela de acesso: Aker Configuration Manager

A janela mostrada acima é a janela principal do Aker Configuration Manager e é a partir dela que se tem acesso a todas as opções de configuração, inclusive da ativação da licença do produto. Sem ativação da licença não será possível realizar as configurações subsequentes.

A interface Remota é composta de 3 menus descritos brevemente abaixo (quando existe um Aker Configuration Manager selecionado, um quarto menu é mostrado com opções específicas para o mesmo):

Opções

O menu ***'Opções'*** contém as configurações relacionadas ao layout da Interface Remota.

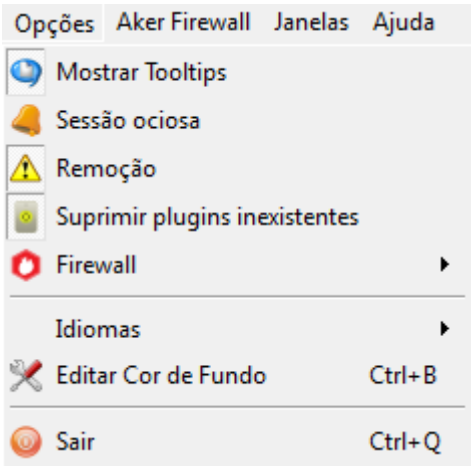

Figura 11 – Opções da Interface Remota

Ao clicar neste menu as seguintes opções serão exibidas:

- **Mostrar Tooltips:** é uma dica de contexto. É aquela moldura pop up que abre quando você passa o mouse sobre um elemento HTML (normalmente uma palavra em um texto) e que contém uma explicação adicional sobre aquele elemento que recebeu o ponteiro do mouse sobre ele.
- **Sessão ociosa:** Permite definir o tempo máximo, em minutos, que a interface permanecerá conectada ao Aker Configuration Manager sem receber nenhum comando do administrador. Assim que este tempo limite for atingido, a interface automaticamente será desconectada do Aker Configuration Manager, permitindo que uma nova sessão seja estabelecida. Seu valor pode variar entre 1 e 60. A caixa '***Sem limite'*** quando estiver marcada não desconectará a interface do Aker Configuration Manager. O Valor padrão é de 1 minuto. Após realizar as alterações clique no botão ***'OK',*** caso não realize nenhuma alteração, clique no botão ***'Cancelar'.***

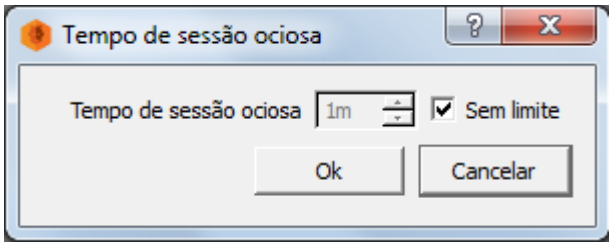

Figura 12 – Tempo de sessão ociosa

- **Remoção:** Caso deseje remover alguma regra, filtro, etc, será enviado uma mensagem com um a pergunta se deseja realmente remover o item selecionado;
- **Suprimir plugins inexistentes:** caso não tenha um plugin da Aker instalado, ao clicar nessa opção, será mostrada a mensagem do que está faltando.
- **Firewall:** este menu para cadastrar mais firewalls na Interface Remota de modo que possibilite simultaneamente a administração de diversos Aker Firewalls. Com a interface conectada a mais de um firewall simultaneamente, é possível usar a facilidade de arrastar e soltar as entidades e regras entre firewalls, de modo a facilitar a replicação de determinadas configurações entre eles. Dentro do menu Firewall, tem-se:

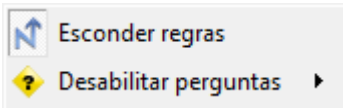

Figura 13 - Opção para a exibição das regras

- Esconder regras: colapsa as políticas de regra;

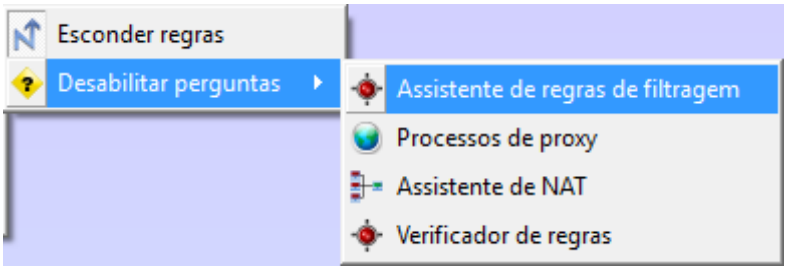

Figura 14 – Desabilitar perguntas da Interface Remota

Desabilitar perguntas

- **Assistente de regras de filtragem:** assistente para a criação de regras de filtragem;
- Assistente de Nat: cria regras de Nat;
- **Verificador de regras:** checagem das regras de filtragem para verificar se não há regras sobrepostas;

- **Idiomas:** é possível escolher em qual idioma deseja acessar a Interface Remota (Inglês ou Português);

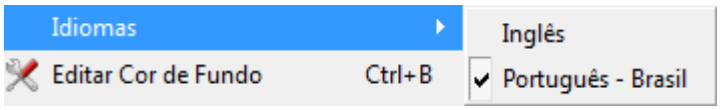

Figura 15 – Opções de idiomas da Interface Remota

- **Editar cor de fundo:** é possível escolher com qual cor de fundo deseja-se trabalhar. Posteriormente serão dados maiores explicações;

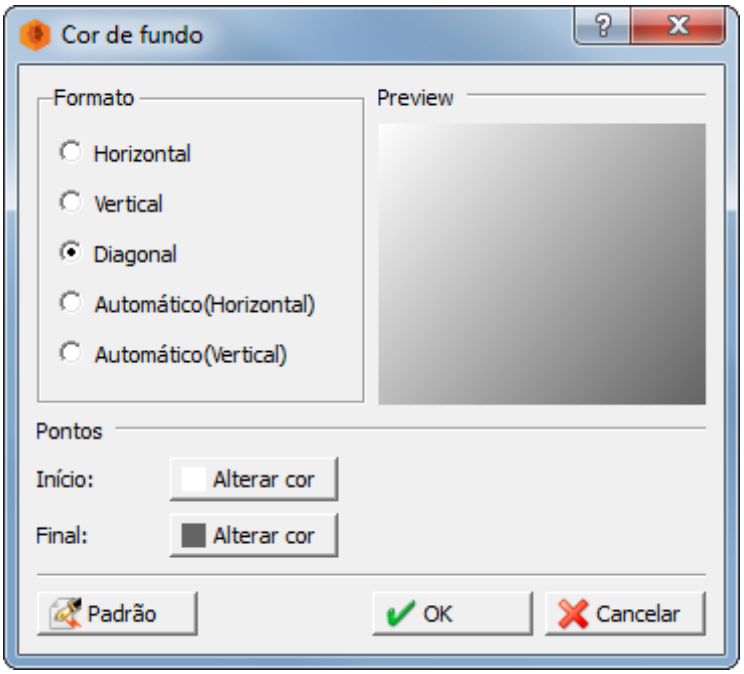

Figura 16 – Alterando a cor de fundo da Interface Remota

- **Sair:** Quando selecionada a opção sair surgirá à mensagem abaixo:

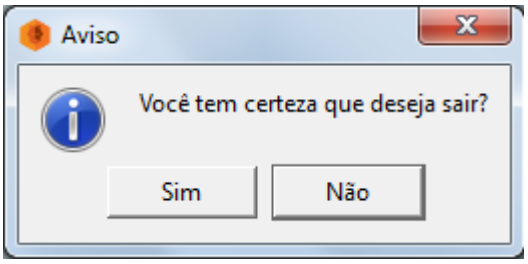

Figura 17 – Mensagem ao sair da Interface Remota

Se clicar no botão ***'Sim'*** a Interface Remota será fechada, se clicar no botão '***Não',*** a interface continua aberta.

Janelas

O Menu "Janelas" possui as funções de configuração das janelas abertas e da barra de menu.

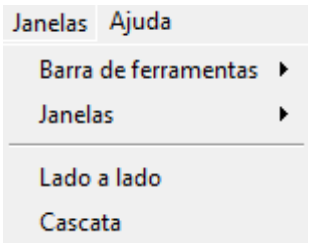

Figura 18 - Menu Janelas

- **Barra de ferramentas:** esta opção permite definir se a barra de ferramentas na parte superior da janela principal será mostrada ou não.

- **Janelas:** mostra o item de dispositivos remotos (essa opção também pode ser acessada pressionando o botão do teclado ***'F9'***).

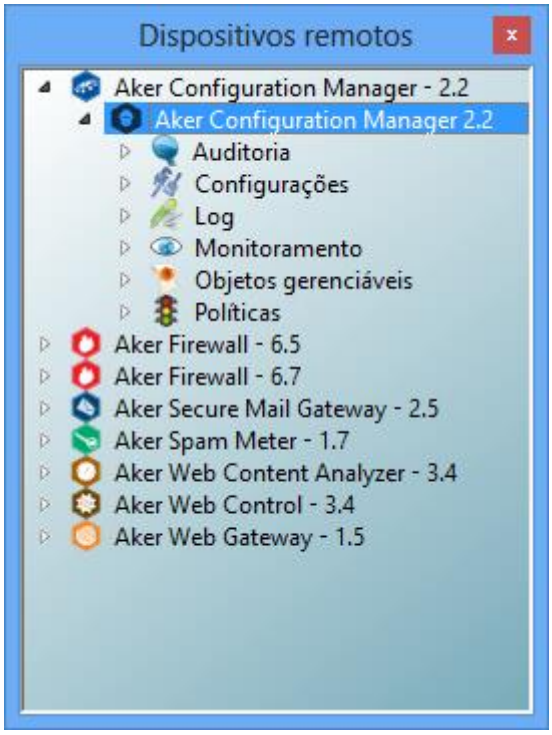

Figura 19 – Dispositivos remotos da Interface remota (Control Center)

- **Entidades:** mostra as entidades (pode também ser acessada pressionando o ***botão 'F9'*** do teclado).

Figura 20 – Janela de Entidades

- **Lado a Lado:** selecionando esta opção, as janelas abertas do lado direito da Interface Remota se ajustam de forma que todas apareceram visíveis.
- **Cascata:** esta opção faz com que as janelas abertas no lado direito da Interface Remota fiquem posicionadas em forma de cascata, uma na frente da outra.

Ajuda:

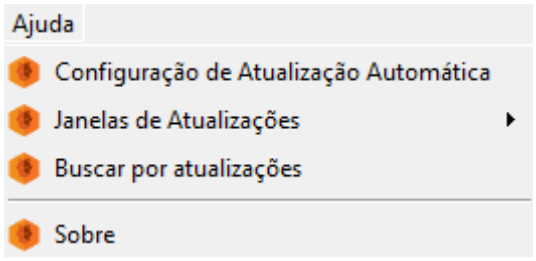

Figura 21 – Menu Ajuda da Interface Remota

- Configuração de atualização automática: permite a configuração automática. Nesta janela é possível 'Habilitar atualização automática', 'Baixar atualizações automaticamente', e 'Habilitar atualizações dos manuais'.

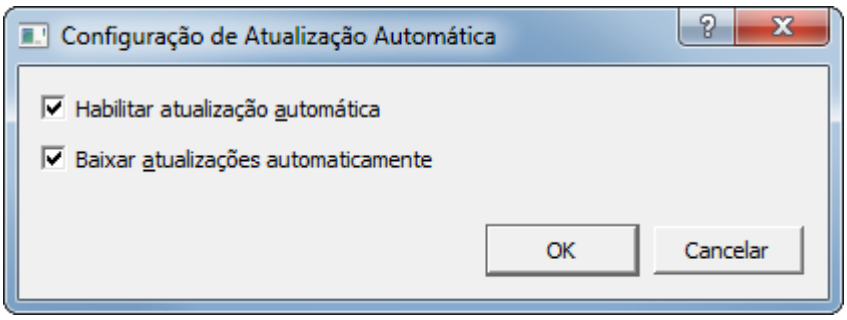

Figura 22 – Opções de configuração de atualização automática

Após escolher as opções desejadas, basta clicar no botão ***'OK'.***

- **Janelas de Atualizações**: neste menu encontram-se os itens Janelas de Downloads que mostram as atualizações que se deseja baixar.

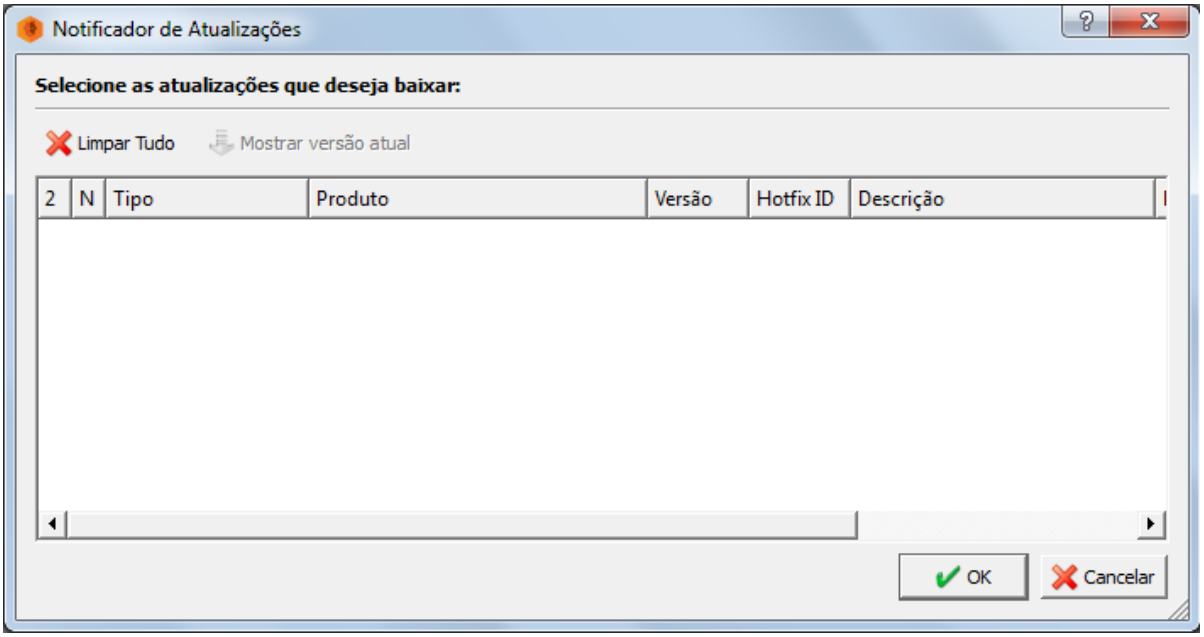

Figura 23 – Notificador de Atualizações

A janela '***Notificador de Instalação de Atualizações'*** permite selecionar as atualizações que se deseja instalar.

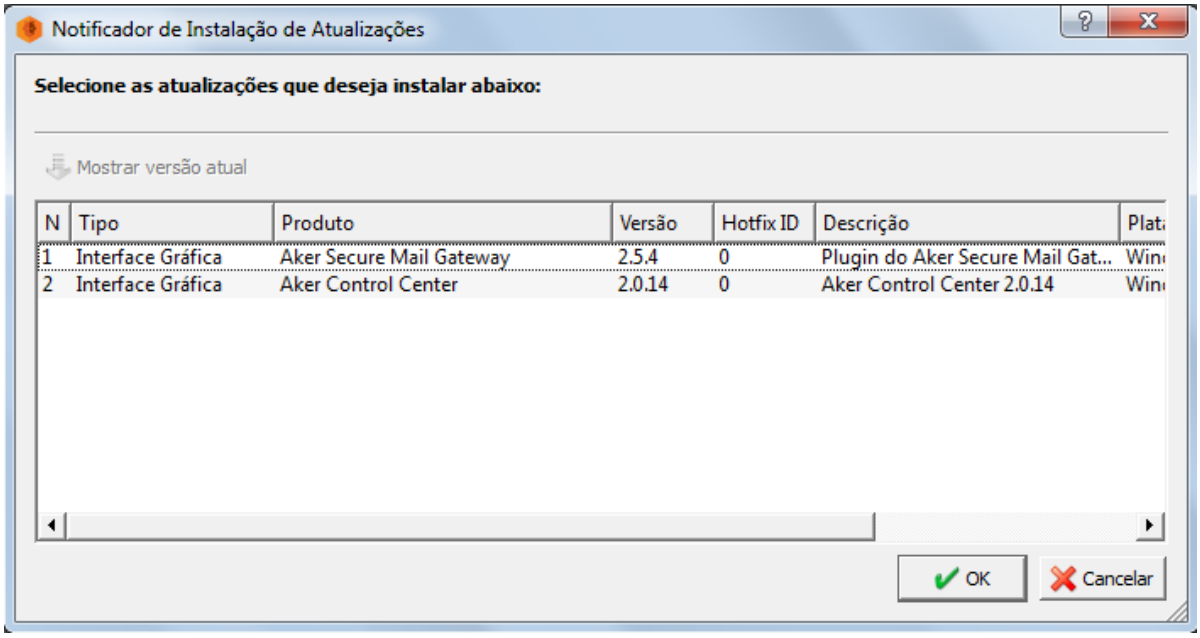

Figura 24 – Notificador de Instalação de Atualizações

- **Busca por atualizações:** Quando selecionada esta opção busca por atualizações pendentes e realizadas, conforme mostra imagem abaixo:

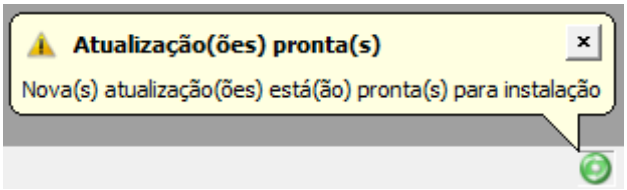

Figura 25 – Atualizações prontas

- **Sobre:** mostra informações sobre o Aker Control Center.

Sobre
Aker Control Center - Versão: 2.0 - Release: 22
Data de compilação: 25 Oct 2013
Na mitologia egípcia, Aker era a personificação da Terra e deus dos mortos. Guardião do portal através do qual o Faraó passava para ir ao mundo espiritual, Aker também provia uma passagem segura para a Barca do Sol. Ele era representado por um par de leões, um de costas para o outro, que olhavam tanto o nascer quanto o pôr do sol.
Aker Control Center Copyrights:
• Este produto utiliza a biblioteca SSL escrita por Eric Young (cay@mincon.oz.au). Copyright © 1995 Eric Young.
• Este utiliza a implementação do algoritmo AES do Dr. B. R. Gladman (brg@gladman.uk.net).
• Este utiliza o algoritmo MD5 da RFC 1321. Copyright © 1991-2 RSA Data Security, Inc.
• Este utiliza a biblioteca de compressão Zlib. Copyright © 1995-1998 Jean-loup Gailly and Mark Adler.
• Este produto utiliza a biblioteca QWT escrita por Josef Wilgen. Copyright © 1997.
Plugin Copyrights >>
Copyright © 1997-2013 Aker Security Solutions. Todos os direitos reservados.
OK

Figura 26 – Informações sobre a Aker Control Center

Para encerrar, clicar no botão ***'OK'.***

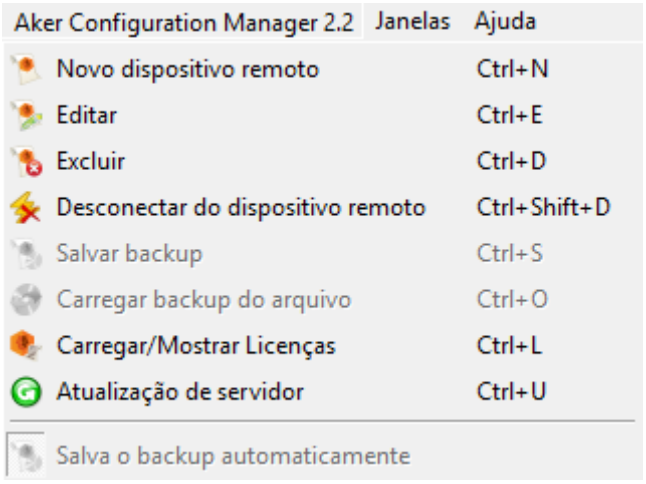

Figura 27 – Menu de Opções do dispositivo remoto

Inicialmente nem todas as opções dos menus se encontram habilitadas, por funcionarem apenas quando houver uma conexão estabelecida. Para ter acesso às demais opções devem estabelecer uma sessão de administração remota com o firewall que deseja administrar. Para tanto se devem seguir os seguintes passos:

Cadastrar o *Configuration Manager* selecionando o menu '***AWC***' (este menu terá o nome que foi escolhido na criação do dispositivo, no caso AWC) opção ***'Novo dispositivo remoto';***

- **Novo Dispositivo Remoto:** Cadastra um novo disposto
- **Editar:** Realiza edições;
- **Excluir**: Apaga o dispositivo selecionado;
- Conectar ao dispositivo selecionado: conecta ao dispositivo;
- **Reiniciar dispositivo:** Reinicia o dispositivo selecionado;
- **Desligar dispositivo**: Desliga o dispositivo remoto;
- **Salva backup automaticamente:** Os backups serão salvos automaticamente.

Ao selecionar o Configuration manager que se deseja conectar;

Clique na opção "*Conectar*" ( ).

- **Textos nos botões:** marcando esta opção será mostrada juntamente com cada ícone a ação correspondente do botão. Desmarcando esta opção, será mostrado apenas o ícone.

- **Dicas para Entidades:** quando esta opção estiver ativada, uma pequena caixa com a descrição de cada entidade irá aparecer quando o mouse for passado sobre seu ícone.

Figura 28 – Informação sobre a Entidade

- **Mostrar ícones nos botões:** esta opção, se ativada, faz com que sejam mostrados ícones nos botões ***'OK'***, ***'Cancelar'*** e ***'Aplicar'*** das janelas.

Cadastrando o Aker Configuration Manager

Nesta seção demonstramos como cadastrar um ou mais firewalls quando selecionamos a opção ***'Novo dispositivo remoto'*** dentro do menu ***'AWC'*** ou no ícone ***'Criar dispositivo remoto'*** (*).*

Aparecerá a seguinte janela ***'Editar Dispositivo remoto'***. Nessa janela, é possível escolher o tipo de autenticação desejada. De acordo com cada opção a janela será alterada, mostrando os campos correspondentes.

Aparecerá a seguinte janela ***'Editar Dispositivo remoto'***. Nessa janela, é possível escolher o tipo de autenticação desejada. De acordo com cada opção a janela será alterada, mostrando os campos correspondentes.

Tipo de Autenticação: Usuário/Senha

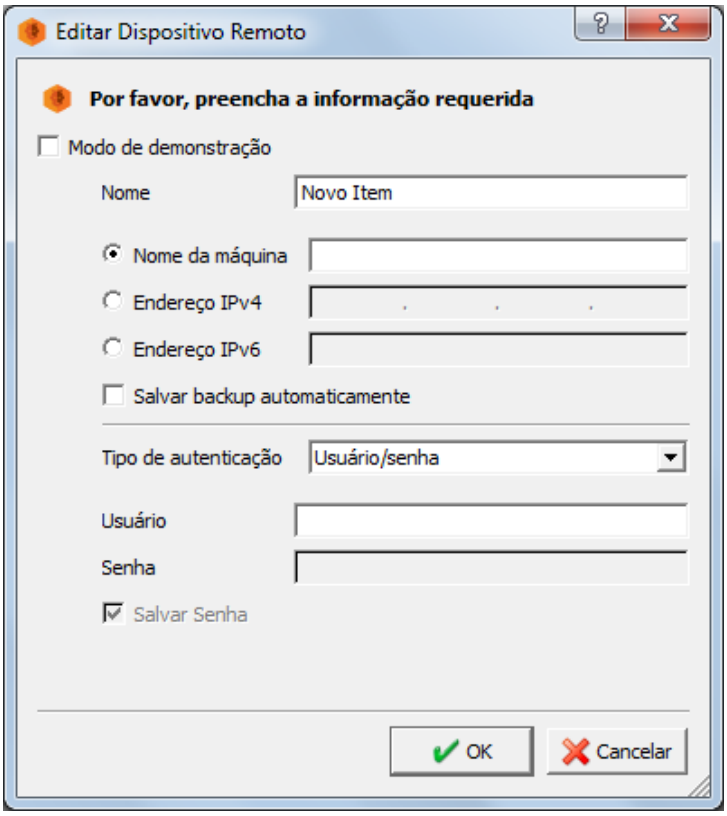

Figura 29 – Tipo de Autenticação (Usuário e senha)

Modo de demonstração: Quando selecionada essa opção, será criado um Configuration Manager de demonstração com uma configuração padronizada. Nenhuma conexão real será feita ao tentar se conectar neste Configuration Manager, podendo-se criar quantos Configuration Managers de demonstração for desejado, cada um com a configuração distinta um do outro;

Nome: cadastrar o nome pelo qual o Configuration Manager será referenciado na Interface Remota;

Nome da máquina: Caso o servidor do Configuration Manager no qual se deseja conectar possua um nome associado ao IP da máquina, basta colocar este nome nesta opção para que o Control Center resolva o DNS automaticamente e se conecte no servidor;

Endereço IPv4 e IPv6: cadastra o endereço IP para conectar no Aker Configuration Manager;

Usuário: esse campo identifica o usuário que acessará o Aker Configuration Manager. Este campo grava os usuários que acessam o Aker Configuration Manager, permitindo posterior reutilização.

Senha: a senha do usuário. Caso deixe a caixa ***'Salvar Senha'*** marcada, não será necessário digitar a senha quando fizer a conexão (a senha aparecerá na tela como vários asteriscos' *'). Caso ela esteja desmarcada, este campo ficará desabilitado.

Parte superior do formulário

A cada 3 tentativas inválidas, o cliente é bloqueado de acessar a Control Center por 3 minutos. A cada tentativa inválida gera-se um evento 'Excesso de tentativas invalidas' do módulo Daemons do Aker Configuration manager.

No final basta clicar em ***'OK'*** e o Aker Configuration Manager estará cadastrado, como o tipo de autenticação selecionado. No caso de cancelar o cadastro do Aker Configuration Manager, basta clicar em ***'Cancelar'.***

Tipo de Autenticação: X.509

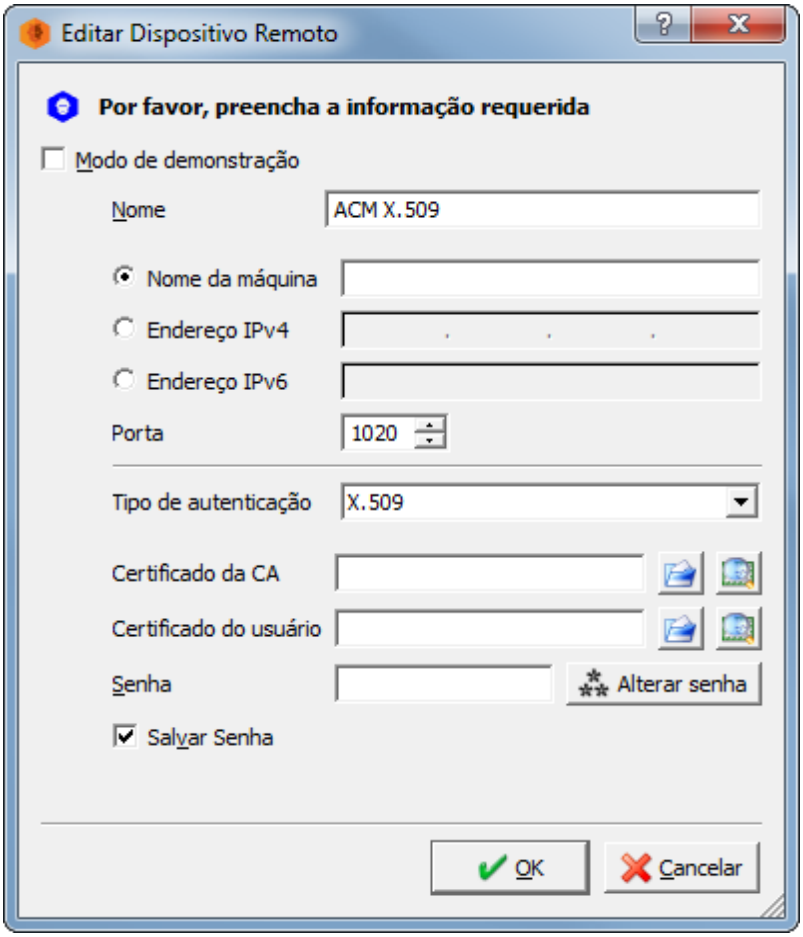

Figura 30 - Tipo de Autenticação (X.509)

Essa opção permite autenticação com certificação digital X509.

Certificado da CA: representa o certificado raiz da autoridade certificadora, mostra o Domínio (C.N) desse certificado.

Ao clicar no ícone mostrado abaixo, carrega-se um arquivo com extensão '*.cer/*.crt' que contém o certificado.

Figura 31 – Ícone: Carregar certificado

O ícone a seguir, mostra um resumo das informações do certificado.

Figura 32 – Ícone: Informações do certificado

Certificado do Usuário: essa opção permite carregar um pacote de certificado no formato ***PKCS#12***. Ele desmembra o pacote em dois arquivos, um com o certificado e outro com a chave. Carrega um certificado com uma senha e a outra senha é para salvar o arquivo da chave, salvando assim, de forma encriptada.

Senha: Senha com a qual a chave primária foi salva. Se informar (cadastro), decifra a chave e manda para o Aker Configuration Manager fazer a autenticação. Caso deixe a caixa ***'Salvar Senha'*** marcada, não será necessário digitar a senha quando fizer a conexão (a senha aparecerá na tela como vários asteriscos '*'). Caso ela esteja desmarcada, este campo estará desabilitado.

Alterar Senha: Altera a senha cadastrada no campo senha.

Salvar Senha: Permite que a senha seja salva automaticamente.

Tipo de Autenticação: Agente externo

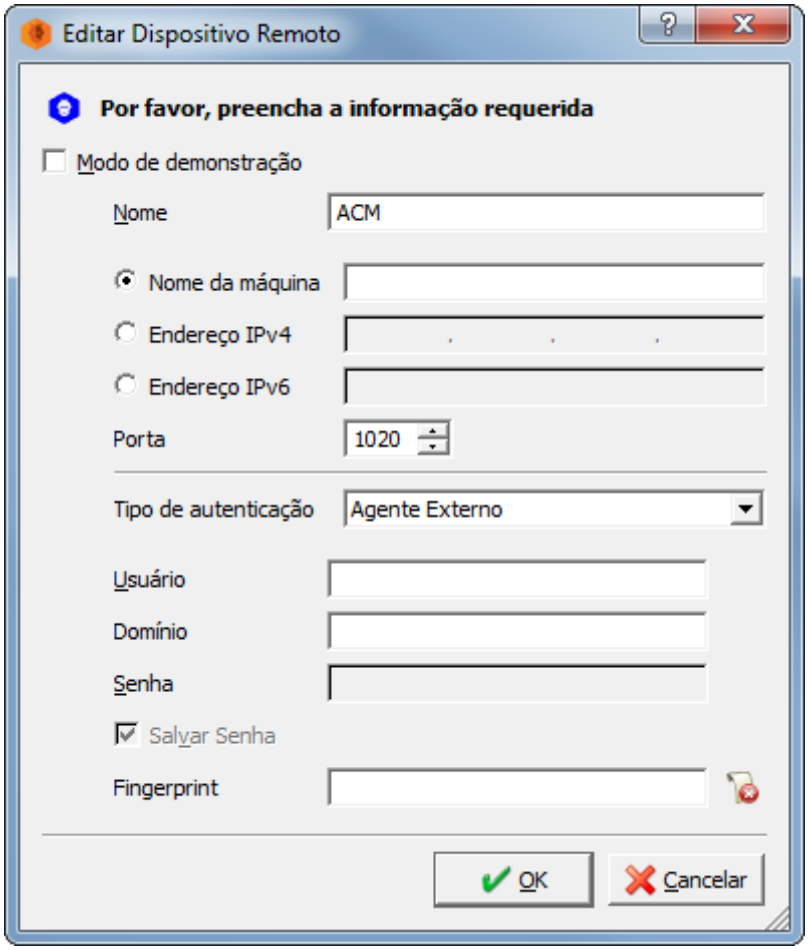

Figura 33 - Tipo de Autenticação (Agente externo)

Essa opção permite autenticação por meio de ***Agentes Externos.***

Usuário: O usuário que acessará o Aker Configuration Manager. Este campo grava o usuário, é onde aparecerá todas as vezes que o Aker Configuration Manager for acessado.

Domínio: Nome do domínio no qual o agente externo está rodando

Senha: A senha do usuário. Caso deixe a caixa '***Salvar Senha'*** marcada, não será necessário digitar a senha quando fizer a conexão (a senha aparecerá na tela como vários asteriscos '*'). Caso ela esteja desmarcada, este campo estará desabilitado.

Fingerprint: É um resumo da identificação do certificado digital do Aker Configuration Manager. Essa opção possibilita identificar quando há uma mudança no Agente Externo utilizado, permitindo detectar eventuais fraudes.

Na primeira vez que há a tentativa da conexão não haverá a identificação do Aker Configuration Manager. A partir da segunda vez todas às vezes que é conectado vai comparar com o fingerprint.

Apagar Fingerprint: Zera e começa do estado inicial. Se há uma troca de Configuration Manager a identificação será diferente, então não será possível à conexão, somente se clicar no ícone apaga fingerprint ( ).

Depois de cadastrarmos o Configuration Manager, pode-se clicar duas vezes no ícone criado para este, no lado esquerdo da janela, ou clicar uma vez para selecioná-lo e, em seguida, no botão ***'Conectar'*** .

5.4 Finalizando a administração remota

Existem três formas de finalizar a administração remota do Aker Configuration Manager:

Finalizando a sessão clicando com o botão direito do mouse no Configuration Manager conectado e selecionando ***'Desconectar do dispositivo remoto'***;

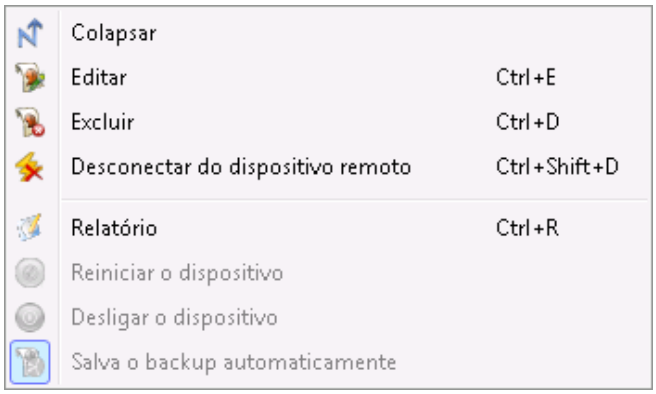

Figura 34 – Finalizando a administração remota

Clicando em ***'Desconectar do dispositivo remoto'*** na barra de ferramentas ou fechando a Interface Remota. Neste caso você perderá a conexão com todos os Configuration Managers que estiverem conectados.

Caso queira sair do programa, deve-se clicar no botão ***'Sair'***, na barra de ferramentas da janela principal ou clicar no ***'x'*** no canto superior direito da janela.

Figura 35 – Botão: Sair

5.5 Ativação de Licença

O Aker Configuration Manager necessita de uma licença válida para seu funcionamento, caso contrário, todas as requisições recebidas pelo servidor serão ignoradas. Antes de iniciar a utilização efetiva do produto é necessário habilitá-lo. Isso é feito através da Licença (ou chave de ativação).

O processo de Ativação da Licença é feito da seguinte maneira:

Aplicação: Habilita o funcionamento do produto por um tempo determinado. A aplicação de novas licenças é feita através do Aker Control Center.

Atualização: Existem duas formas de se atualizar uma licença: uma é a aplicação de uma nova licença, substituindo a licença expirada, e a outra é a atualização somente da data de expiração, sem que seja necessário a geração de uma nova chave de ativação.

Expiração: Antes mesmo de expirar, o Configuration manager envia eventos ao log alertando o usuário sobre a expiração. Ao expirar, todas as requisições recebidas pelo *Partner Engine* serão ignoradas e registradas no log.

A janela Ativação de Licença

Para verificar a licença atual do produto, deve-se clicar no botão ( ) localizado na barra de tarefas no canto superior esquerdo do Control Center. Caso o produto ainda não tenha licença ou se ela estiver expirada, será mostrada uma janela informando que a licença ainda não foi carregada ou ela não existe. Conforme a imagem demonstrada abaixo:

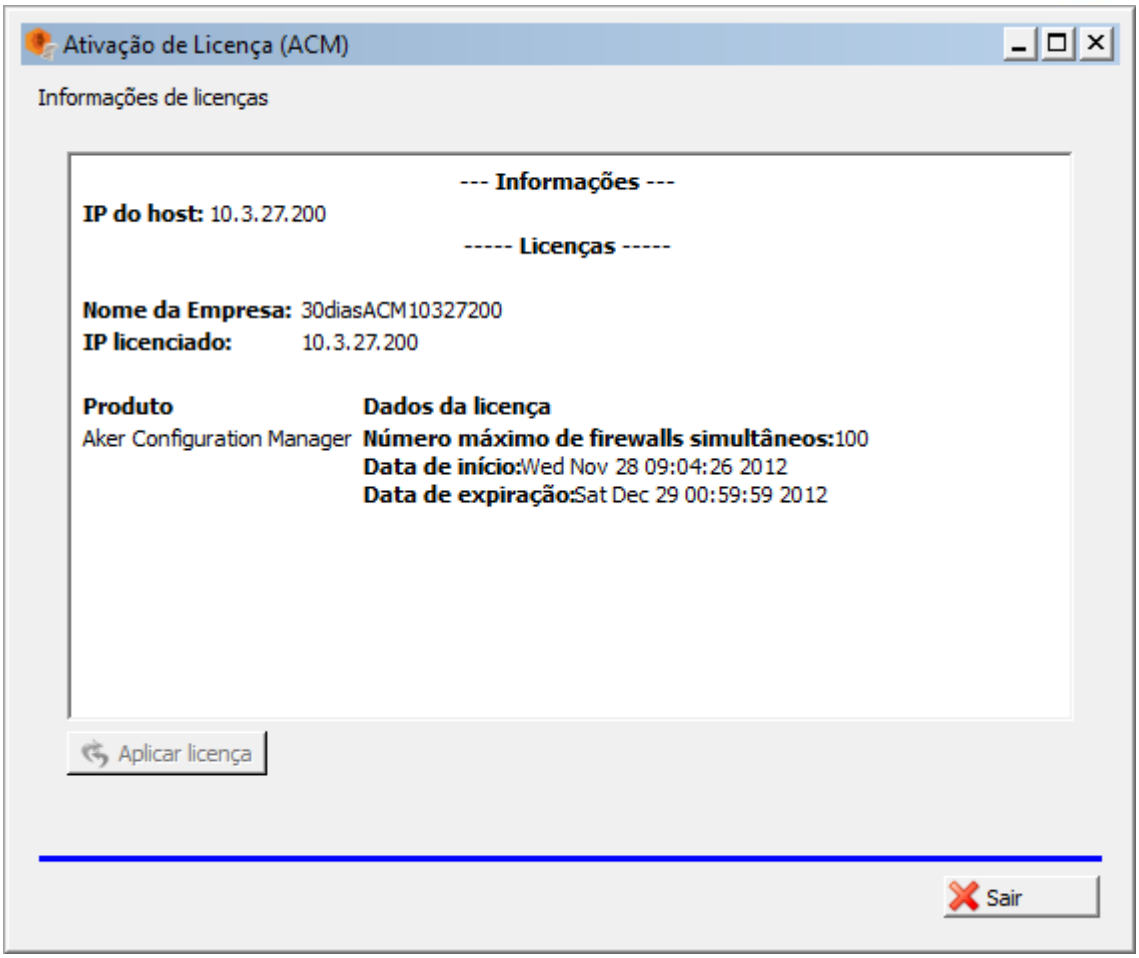

Figura 36 – Ativação de Licença

No exemplo demonstrado acima, o Aker Configuration Manager ainda não está registrado, antes é necessário ativar a licença de uso do produto. Esse procedimento deve ser feito clicando no botão ( ) localizado na barra de tarefas no canto superior da Interface Remota.

Essa opção abrirá um diálogo onde se pode especificar o arquivo de onde a nova chave será carregada. Deve-se selecionar o arquivo no formato ***akk*** (Aker Key).

Janela de escolha de um arquivo para carregar os dados da licença

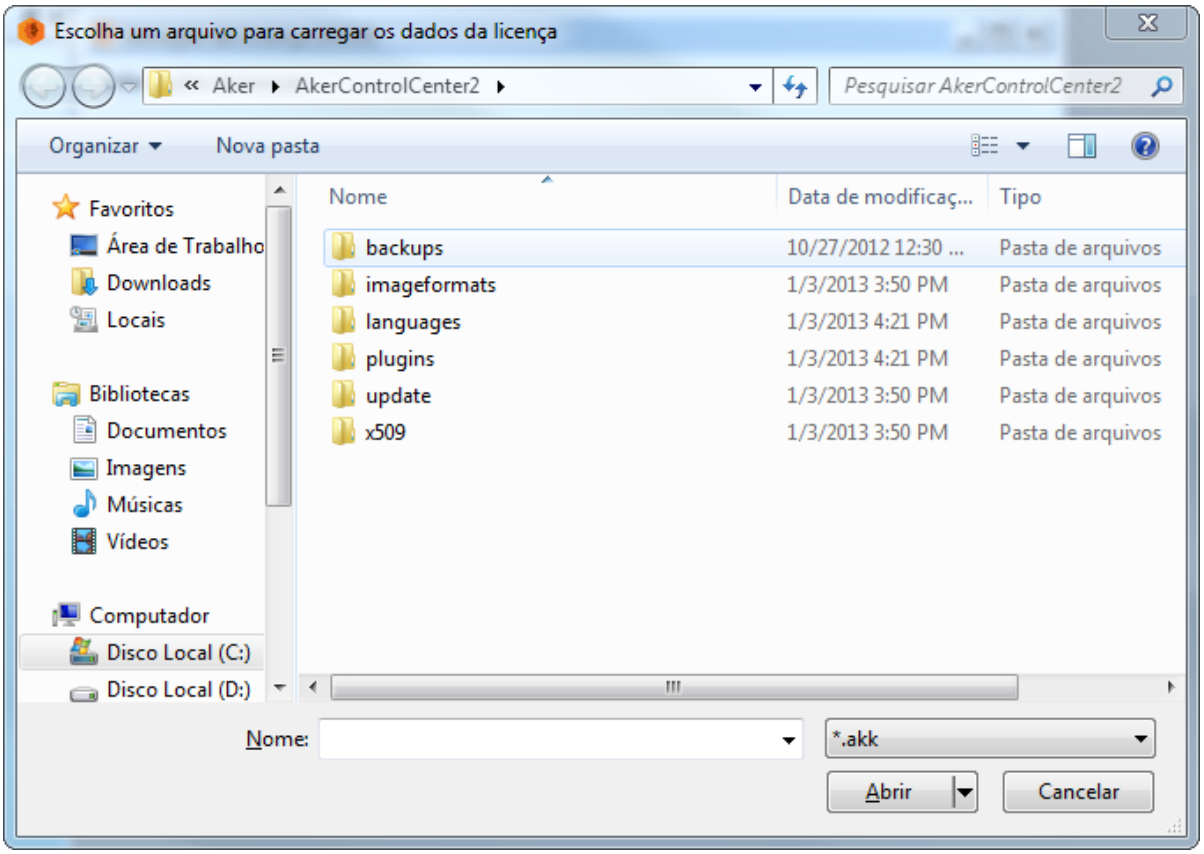

Figura 37 – Janela para carregar os dados da licença

Nesta janela, Selecionar a licença do Aker Configuration Manager e em seguida clique no botão ***Abrir***, caso contrário, clique no botão ***Cancelar*** para desativar a ação. Após concluir esse processo, deve-se confirmar clicando no botão ***Aplicar,*** em seguida no botão ***OK*** da janela de Ativação de Licença.

- O botão **Abrir** fará com que a licença seja carregada e exibida na janela.
- O botão **Cancelar** fará com que a janela seja fechada e a licença não seja carregada.

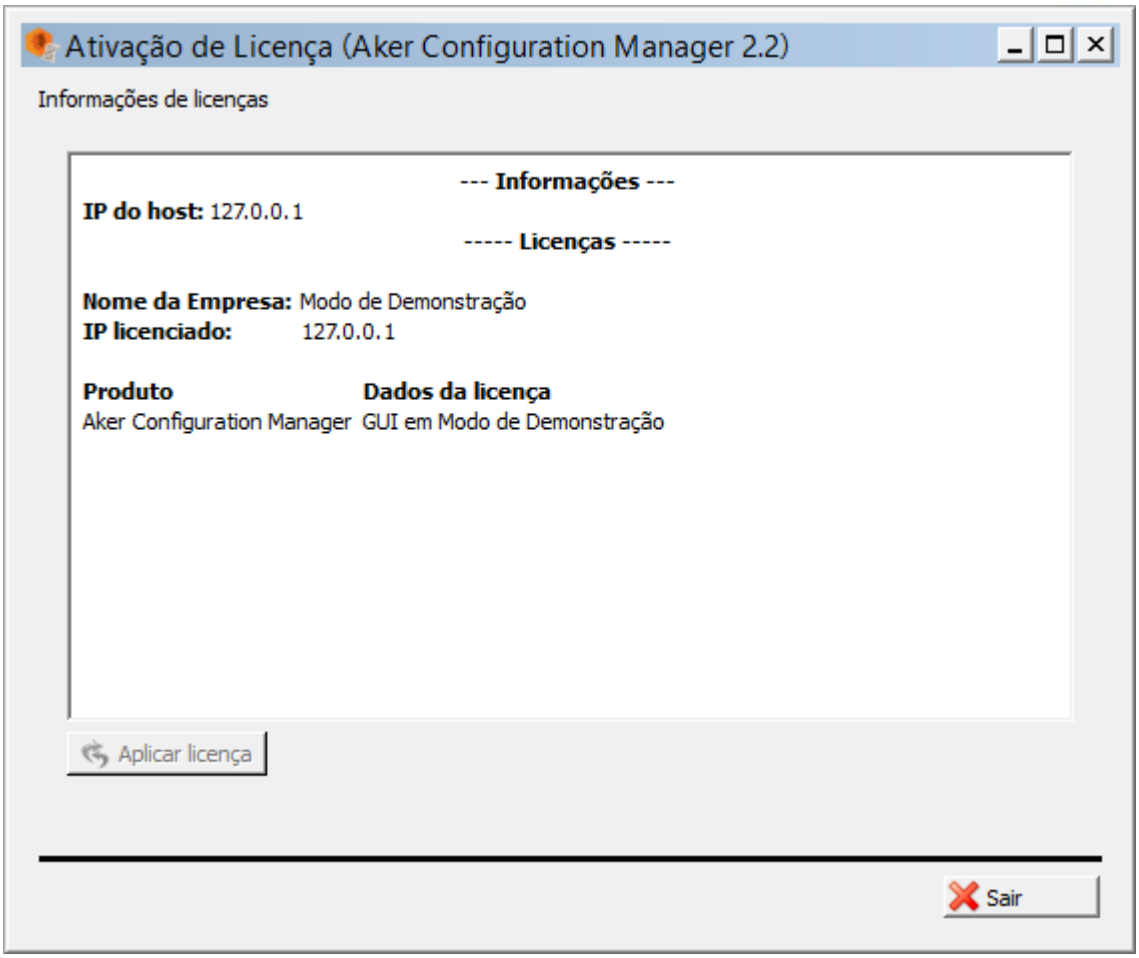

Figura 38 – Ativando a Licença

Depois de aplicada a licença, é mostrado os dados referentes à licença do Aker Configuration Manager. Entre estes dados pode-se verificar o nome da empresa, o IP licenciado, Produto, os dados da licença, data de início e a data de expiração.

- O botão **Aplicar Licença** fará com que as alterações feitas sejam aplicadas e a janela permaneça aberta.
- O botão **Sair** fará com que a janela seja fechada, porém as alterações efetuadas não sejam aplicadas.

5.6 Ativando a licença do Firewall pelo Aker Configuration Manager

Para ativar a licença de um Firewall que esteja sendo gerenciado pelo *Aker Configuration Manager* ferramenta que permite o gerenciamento de vários

Para ativar a licença siga os passos a seguir:

Figura 39 - Objetos gerenciáveis (Status)

- Dentro do Aker Configuration Manager desejado, clique no menu "***Objetos gerenciáveis***";
- Selecione a opção "***Status***";
- A janela a seguir será exibida:

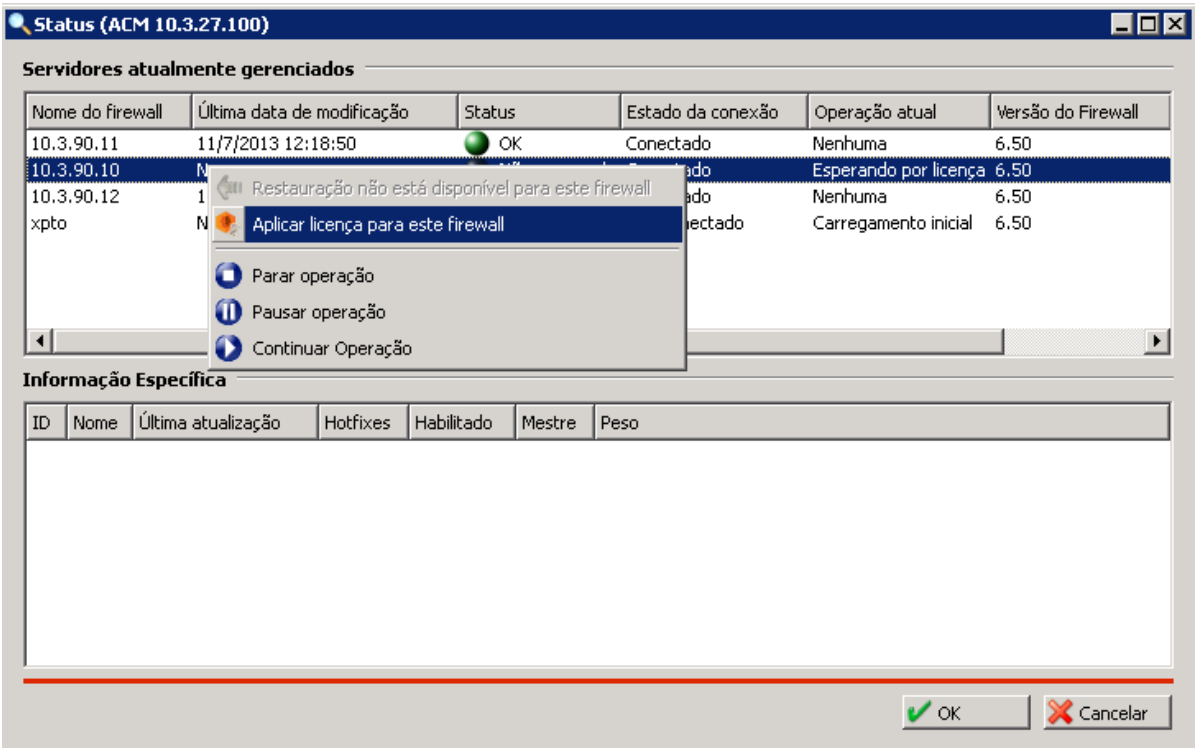

Figura 40 – Janela Status

Esta janela exibe as informações dos Firewalls que são monitorados pelo Aker Configuration Manager, para aplicar a licença se deve:

- Clicar como botão direito do mouse sobre o Firewall desejado, e selecionar a opção "***Aplicar linceça para este firewall***"

A janela a seguir será exibida:

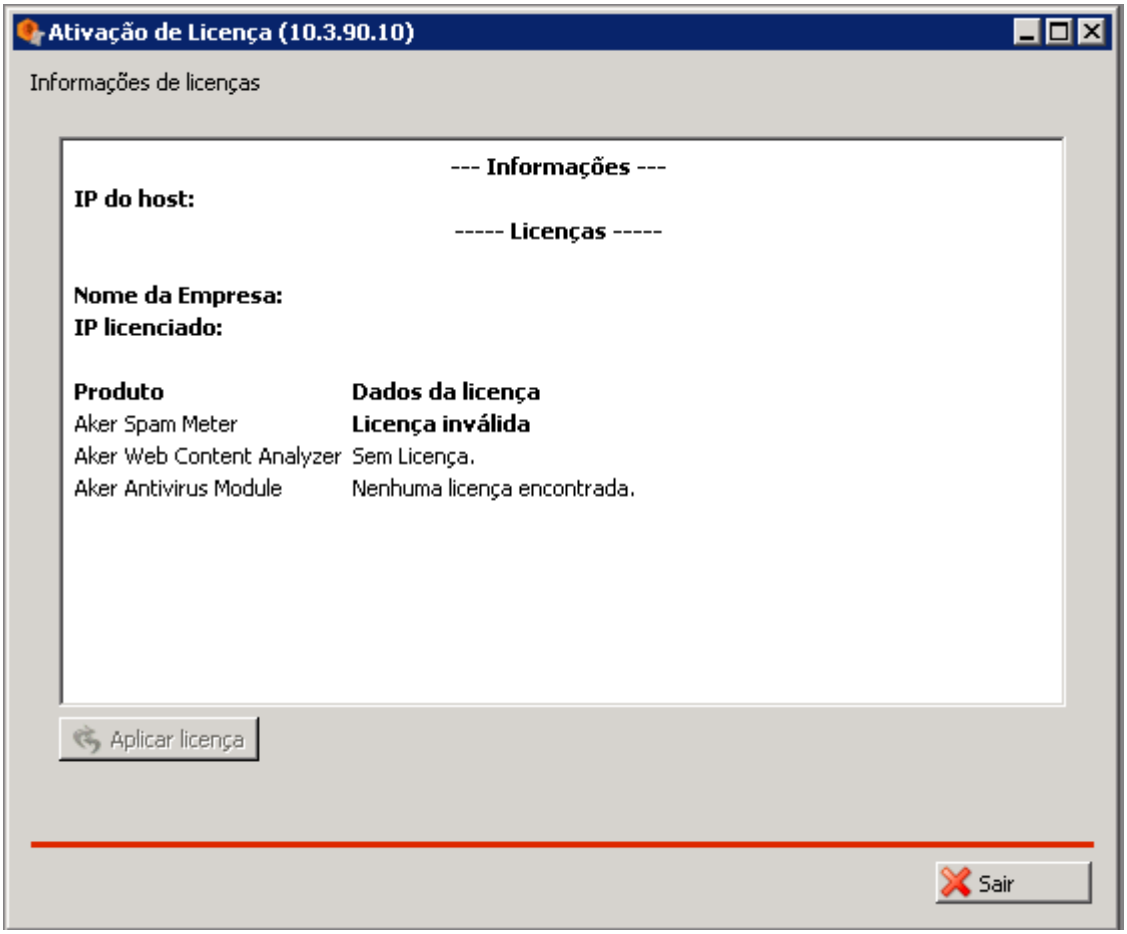

Figura 41 – Janela de ativação de licença

A janela acima será exibida informando o status da licença do produto.

Para carregar a nova licença se deve:

- Clicar no icone (Carregar informação de chave)

A janela a seguir será exibida:

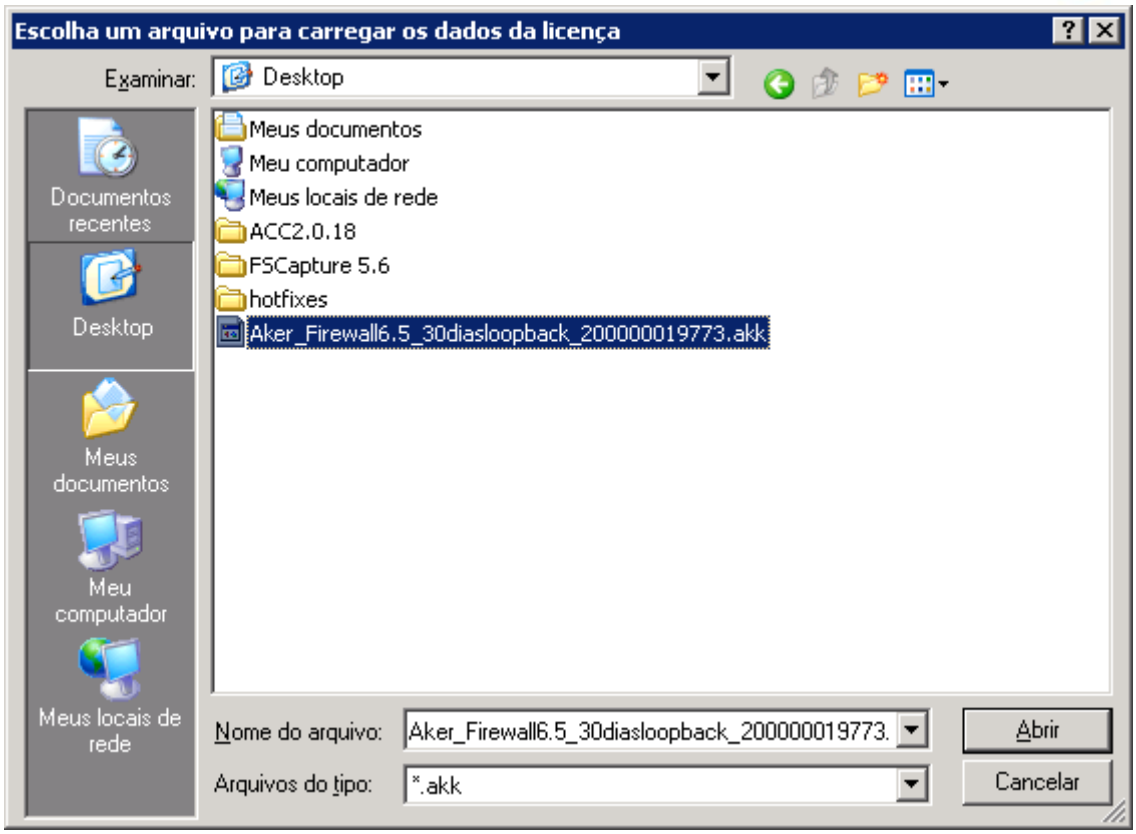

Figura 42 – Janela de localização do arquivo da licença

Nesta janela o usuário deve localizar o arquivo da licença e clicar em "***Abrir***"

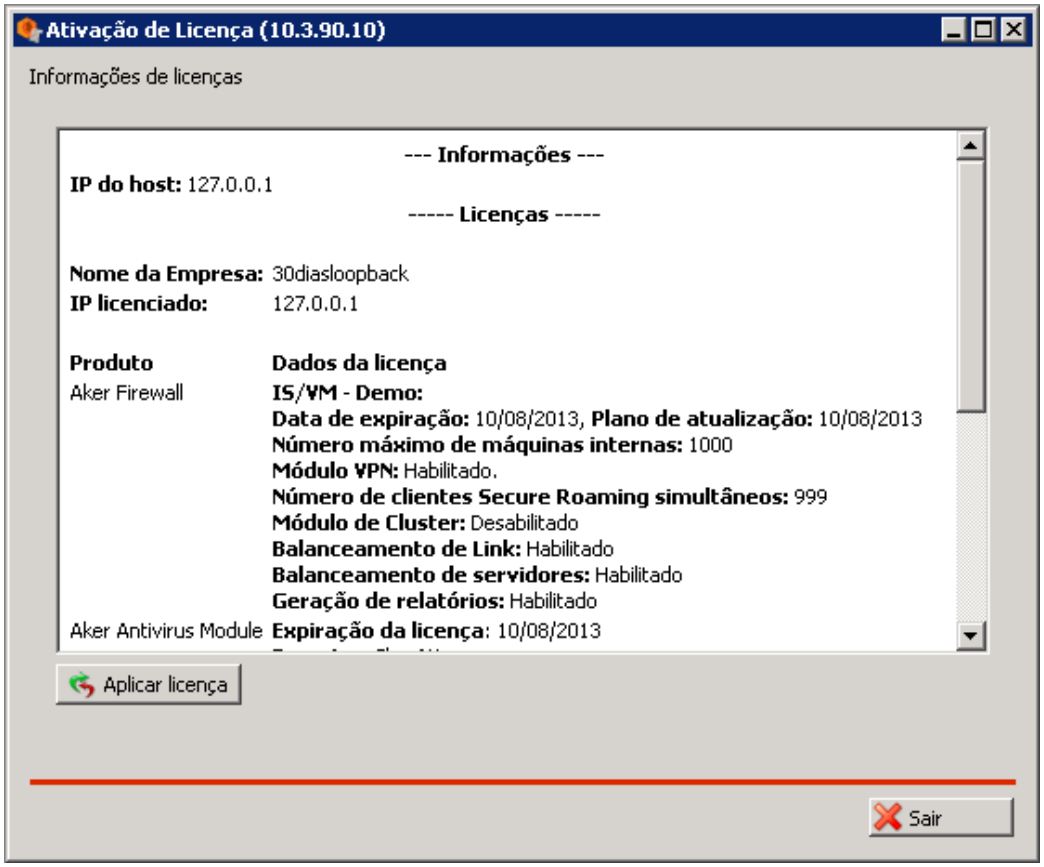

Figura 43 – Janela de ativação da licença

Ao carregar a nova licença a janela acima será exibida, informando as informações da licença.

Para finalizar a ativação, clique em "***Aplicar licença***".

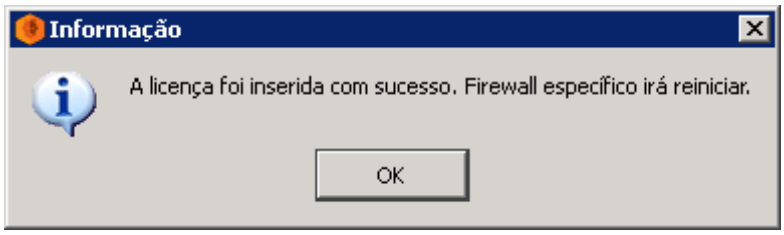

Figura 44 – A licença foi aplicada com sucesso

5.7 Renovação da licença

O processo de 'renovação da licença' é similar ao processo de 'instalação da licença'. O nó mestre irá verificar as licenças de todos os outros *nós,* incluindo os *escravos*, diariamente. Caso algum nó encontre uma licença expirada ou que vá expirar em até 30 dias, a requisição da renovação será feita automaticamente (similar ao processo de instalação mostrado acima). Os dados da licença que já se encontram instalados serão recuperados, e a requisição da renovação da licença será feita automaticamente ao Servidor Externo, que irá gerar um protocolo, e o enviará de volta ao Firewall IS/VM em questão, que então o armazenará para a verificação. A primeira verificação será feita em até 5 minutos. Caso ocorra algum erro à verificação será feita em um período aleatório de até 24 horas *(o usuário deve entrar em contato com o suporte caso à renovação de sua licença não seja efetuada no período de 72h).*

Para cluster o processo de renovação será o mesmo. O nó master fará a requisição ao servidor externo enviando as informações da licença de todos os nós do cluster. A aplicação da primeira licença em um firewall em cluster será feita manualmente. Esta aplicação manual é feita somente nos firewalls que estiverem em cluster.

Faltando 5 dias para que a licença se expire e a renovação da licença não foi efetuada, o usuário deve entrar em contato com o suporte.

5.8 Efetuando as mudanças (commit)

Ao se realizar quaisquer alterações de configuração no Configuration Manager ou em um dos Firewalls que ele gerencia, deve-se salvar essas clicando no ícone ( ) *"Efetuar mudanças"* para que as modificações ocorridas sejam de fato salvas.

Para ter acesso a essa janela basta, clicar no botão ( ) localizado na barra de ferramenta do Configuration Manager.

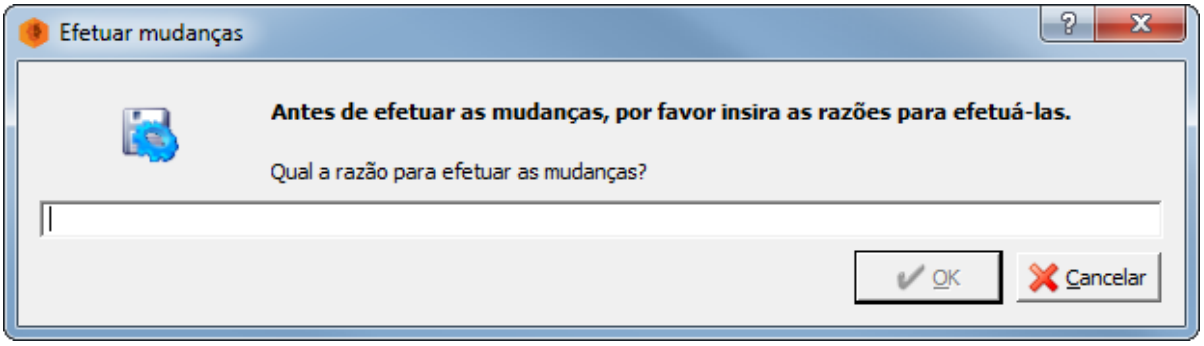
Efetuar mudanças
Antes de efetuar as mudanças, por favor insira as razões para efetuá-las.
Qual a razão para efetuar as mudanças?
OK
Cancelar

Figura 45 – janela de acesso: Efetuar mudanças

5.9 Controlando as Mudanças

Para ter acesso a janela Controle de mudanças, deve-se:

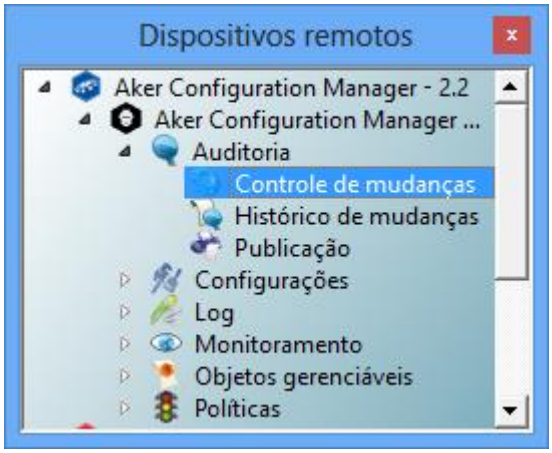

Figura 46 – Auditoria: Controle de mudanças

- Clicar menu *Auditoria*
- Selecionar a opção "Controle de mudanças"

Janela Controle de mudanças

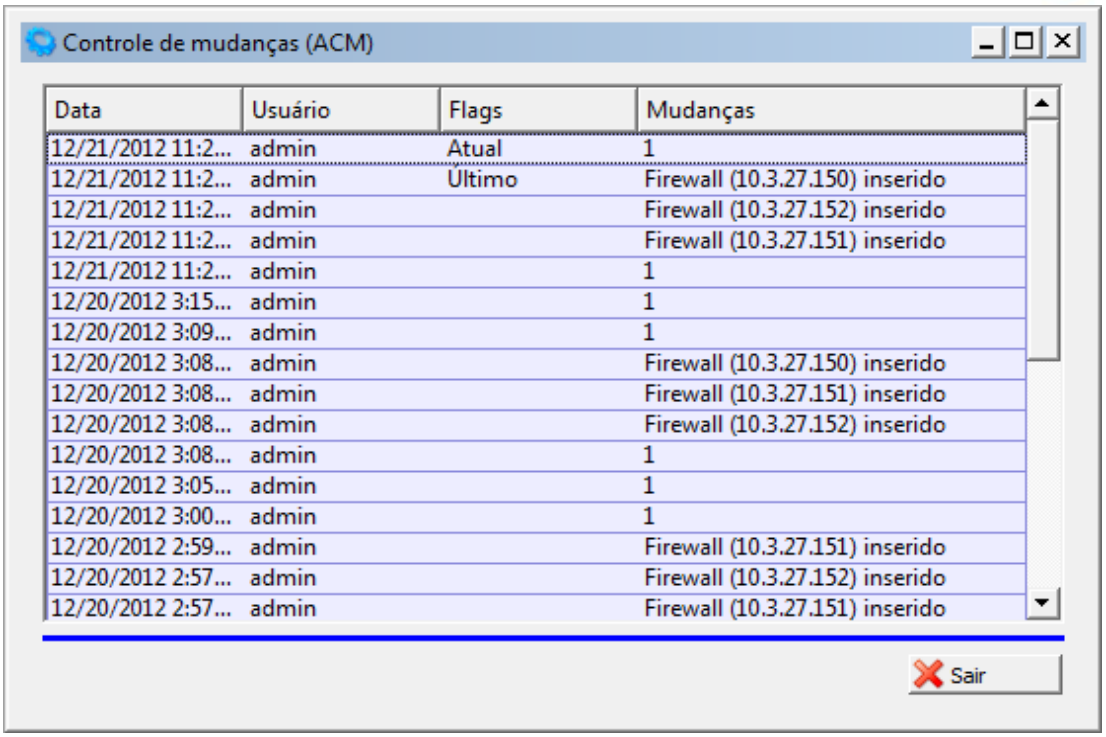
Controle de mudanças (ACM)
Data
Usuário
Flags
Mudanças
12/21/2012 11:2... admin Atual 1
12/21/2012 11:2... admin Ultimo Firewall (10.3.27.150) inserido
12/21/2012 11:2... admin Firewall (10.3.27.152) inserido
12/21/2012 11:2... admin Firewall (10.3.27.151) inserido
12/21/2012 11:2... admin 1
12/20/2012 3:15... admin 1
12/20/2012 3:09... admin 1
12/20/2012 3:08... admin Firewall (10.3.27.150) inserido
12/20/2012 3:08... admin Firewall (10.3.27.151) inserido
12/20/2012 3:08... admin Firewall (10.3.27.152) inserido
12/20/2012 3:08... admin 1
12/20/2012 3:05... admin 1
12/20/2012 3:00... admin 1
12/20/2012 2:59... admin Firewall (10.3.27.151) inserido
12/20/2012 2:57... admin Firewall (10.3.27.152) inserido
12/20/2012 2:57... admin Firewall (10.3.27.151) inserido
Sair

Figura 47 – Janela de controle de mudanças

Esta janela armazena um histórico das diversas configurações feitas no próprio Configuration Manager ou nos Firewalls gerenciados, permitindo que o administrador volte à configuração de todos eles para qualquer estado previamente salvo por ele (isso é tecnicamente uma operação de “rollback”).

Ao clicar com o botão esquerdo sobre uma das configurações ocorridas, será permitido efetuar as seguintes opções. Conforme demonstrada abaixo:

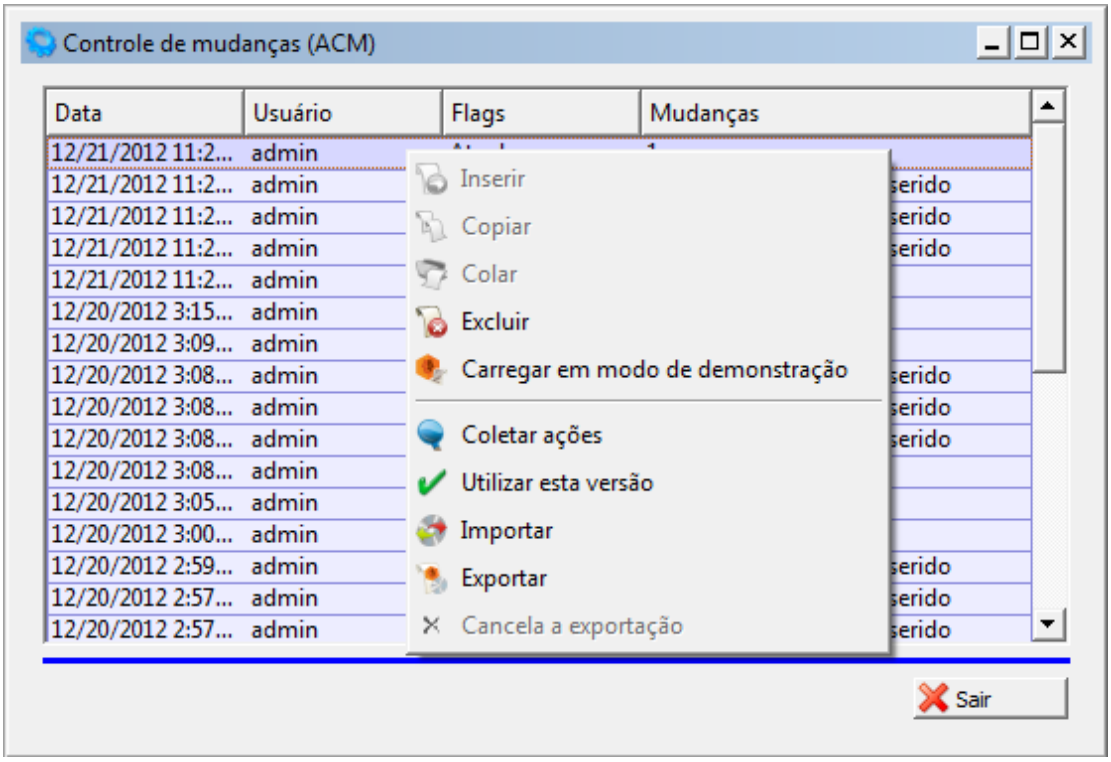

Figura 48 – Opções da Janela de controle de mudanças

Utilizar esta versão: Refaz toda a configuração de acordo com a configuração selecionada.

Importar: permite carregar para o Configuration Manager um arquivo de backup salvo em disco escolhido pelo usuário. Esse arquivo não será imediatamente usado como a nova configuração a menos que o usuário opte por isso.

Exportar: Ao selecionar esta opção, irá salvar o backup em um arquivo escolhido pelo usuário no disco rígido. Quando essa operação estiver ativa, a opção "**Cancelar a exportação**" ficará habilitada.

Histórico **de** mudanças

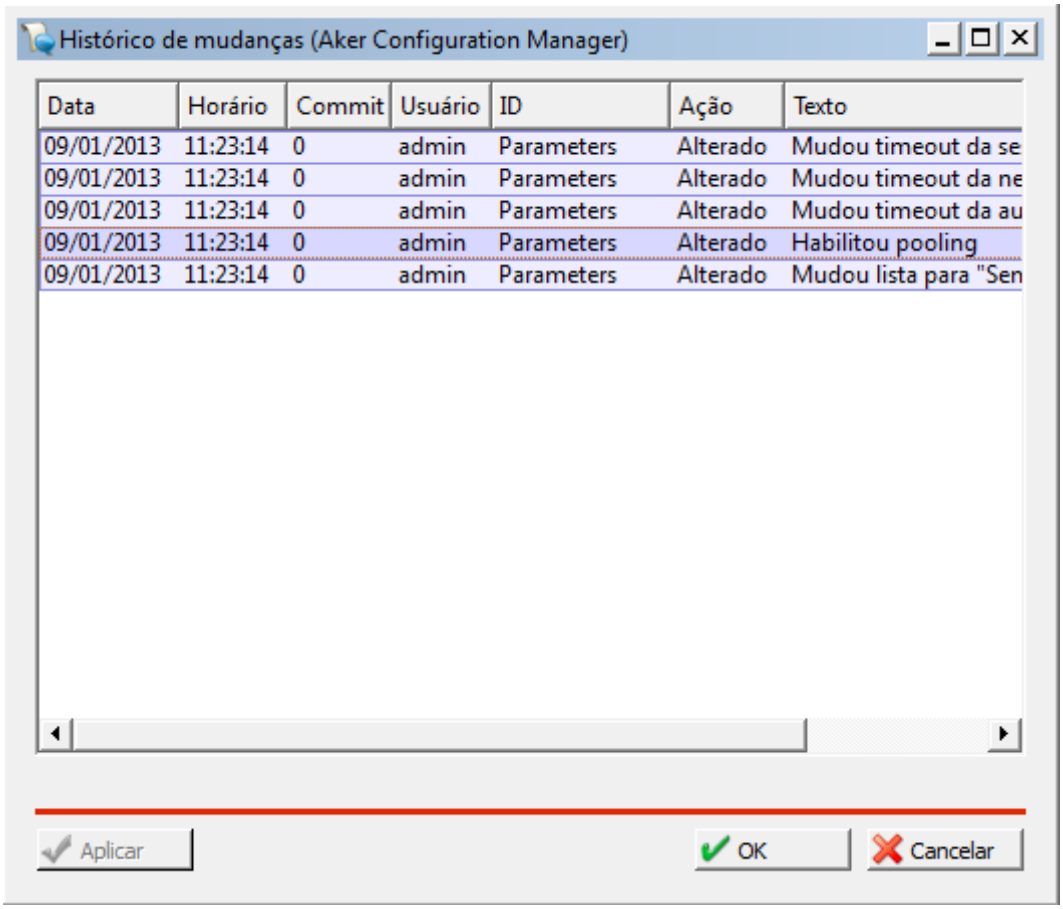
Histórico de mudanças (Aker Configuration Manager)
Data
Horário
Commit
Usuário
ID
Ação
Texto
09/01/2013 11:23:14 0 admin Parameters Alterado Mudou timeout da se
09/01/2013 11:23:14 0 admin Parameters Alterado Mudou timeout da ne
09/01/2013 11:23:14 0 admin Parameters Alterado Mudou timeout da au
09/01/2013 11:23:14 0 admin Parameters Alterado Habilitou pooling
09/01/2013 11:23:14 0 admin Parameters Alterado Mudou lista para "Sen
Aplicar
OK
Cancelar

Figura 49 – Janela de Histórico de mudanças

Esta janela gera eventos de mudanças do Aker Configuration Manager, permitindo que o administrador tenha controle nas alterações que foram efetuadas no Aker Configuration Manager.

Publicação

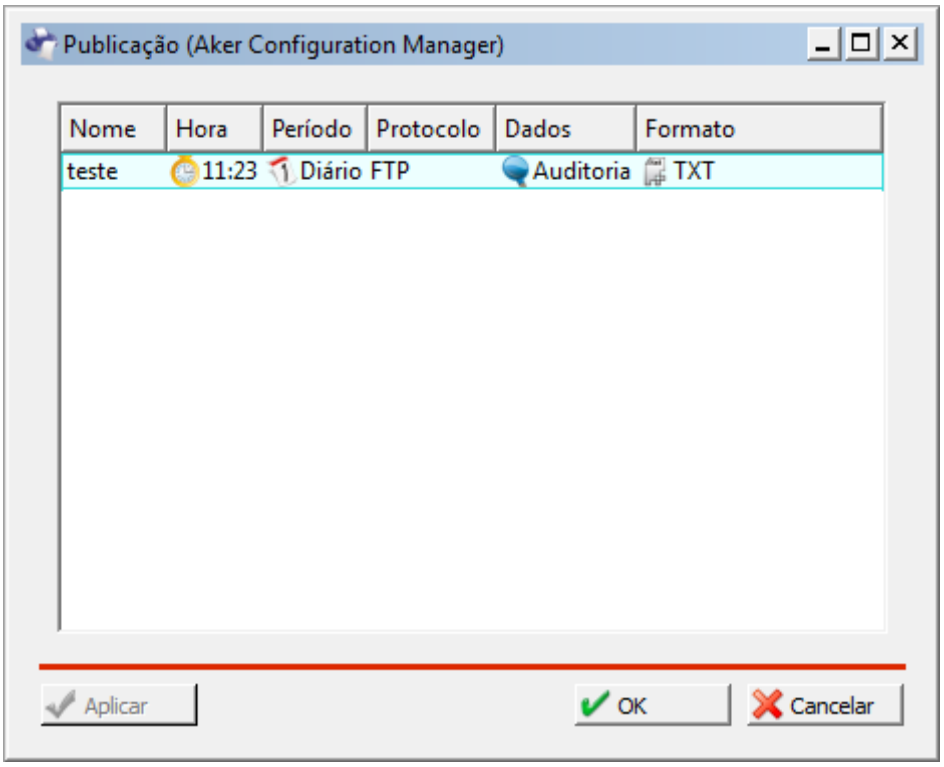

Figura 50 – Janela de Publicação

Esta janela exporta os logs e auditorias que foram aplicadas no *Aker Configuration Manage*r para um servidor FTP, em formato TXT, PDF ou HTML. Estas publicações podem ser feitas diariamente, semanalmente ou mensalmente.

Para ter acesso a janela de opções de publicação, clique com o botão direito dentro da janela de Publicação, e escolha a opção *Inserir*. A janela a seguir será exibida:

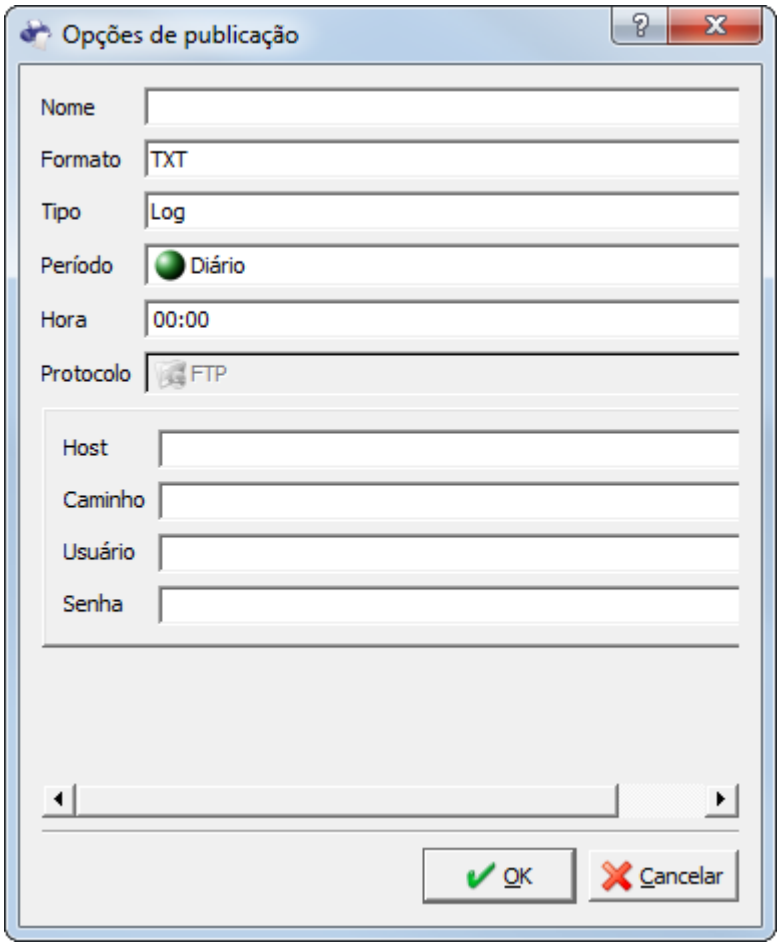

Figura 51 – Opções de publicação

Administrando Usuários
Do
Aker Configuration Manager

6 Administrando Usuários do Aker Configuration Manager

Neste capítulo mostraremos como criar os usuários que irão administrar remotamente o Aker Configuration Manager.

Quem são os usuários do Aker Configuration Manager?

Para que algum usuário consiga administrar remotamente o Aker Configuration Manager, é preciso ser reconhecida e validada pelo sistema.

Esta validação é feita na forma de senhas, sendo que cada um dos administradores deverá ser previamente cadastrado com um login e uma senha, já definindo as suas atribuições.

Além disso, o **Aker Configuration Manager** permite a existência de vários administradores distintos, cada um responsável por uma determinada tarefa da administração. Isso, além de facilitar a administração, permite um maior controle e uma maior segurança.

6.1 Utilizando a Interface Remota

Para ter acesso à janela de administração de usuários, na interface remota deve-se:

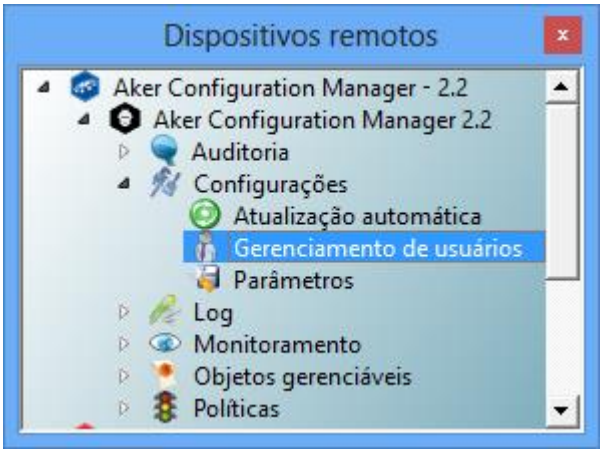

Figura 52 – Configurações: Gerenciamento de usuários

- Clicar no menu *Configurações*
- Selecionar a opção Gerenciamento de usuários

Esta opção só estará habilitada se o usuário que estiver com a sessão aberta na interface remota, tiver autoridade para gerenciar usuários. Isso será comentado em detalhes no próximo tópico.

A janela Administração de Usuários

Aba Usuários Internos

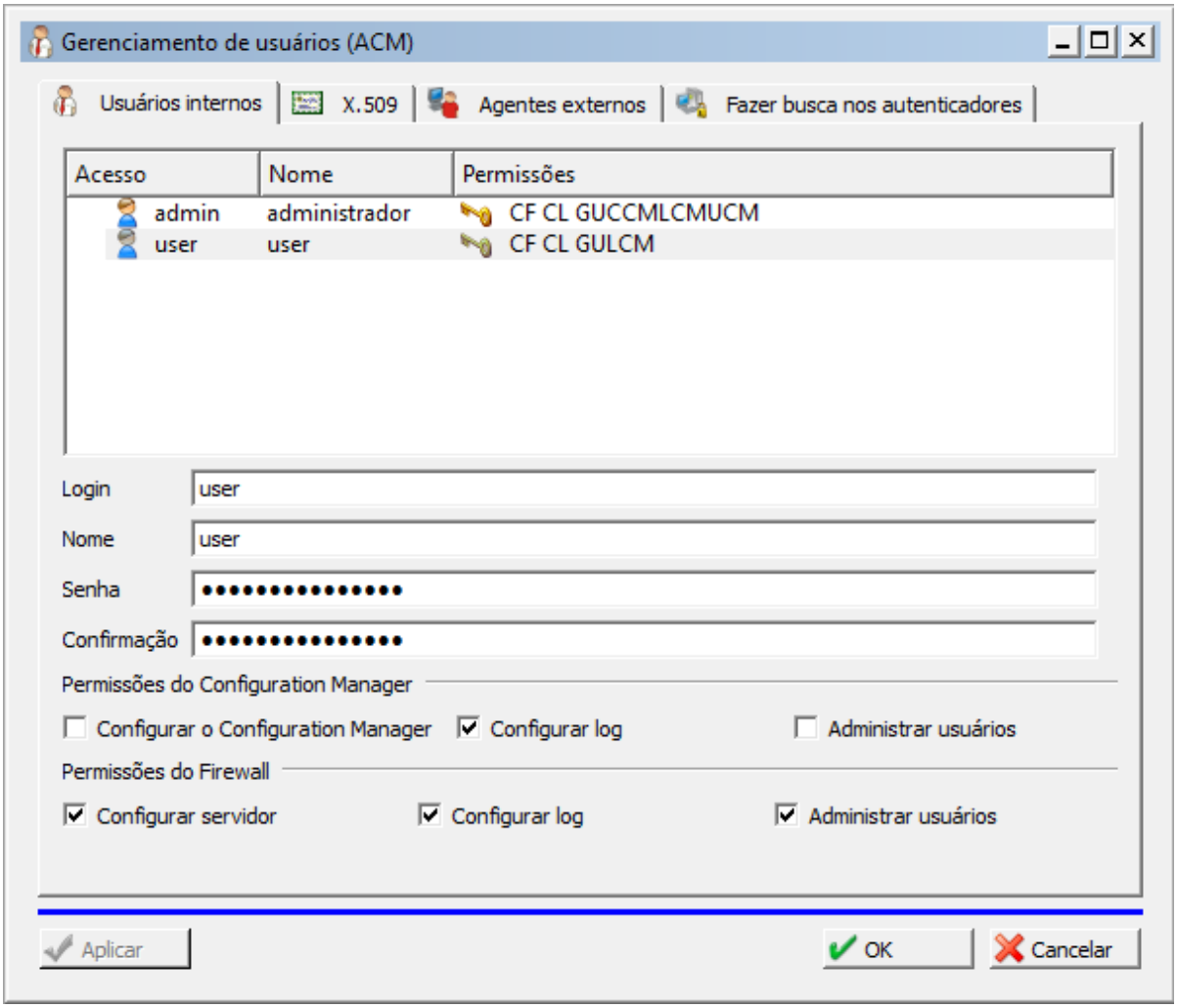

Figura 53 – Aba Usuários internos

Esta janela consiste de uma lista de todos os usuários atualmente definidos para acesso à administração do Aker Configuration Manager. Para cada usuário, é mostrado seu login, seu nome completo e suas permissões.

- O botão **OK** fará com que a janela de administração de usuários seja fechada e as modificações salvas.
- O botão **Aplicar** fará com que as alterações realizadas sobre um determinado usuário sejam aplicadas, isto é, realizadas permanentemente, sem fechar a janela.
- O botão **Cancelar** fechará a janela de administração de usuários e descartará todas as alterações efetuadas.

Quando um usuário for selecionado, os seus atributos completos serão mostrados nos campos Permissões.

Para alterar os atributos de um usuário, deve-se proceder da seguinte forma:

1. Selecionar o usuário a ser alterado clicando sobre seu nome com o botão esquerdo do mouse. Neste momento serão mostrados os seus atributos nos campos após a listagem de usuários.
2. Alterar o valor dos atributos desejados e Clicar no botão **Aplicar** ou no botão **OK**. A partir deste momento as alterações serão efetivadas.

Para incluir um usuário na lista, deve-se proceder da seguinte forma:

1. Clicar com o botão direito do mouse em qualquer lugar da área reservada para mostrar a lista e selecionar a opção Incluir no menu pop-up ou clicar no ícone ( ) que representa a inclusão na barra de ferramentas.
2. Preencher os campos do usuário a ser incluído e Clicar no botão **Aplicar** ou no botão **OK**.

Para remover um usuário da lista, deve-se proceder da seguinte forma:

1. Selecionar o usuário a ser removido, clicando sobre seu nome com o botão esquerdo do mouse e clicar no ícone ( ) que representa a remoção na barra de ferramentas.

Ou

2. Clicar com o botão direito do mouse sobre o nome do usuário a ser removido e selecionar a opção **Remover** no menu pop-up.

Significado dos atributos de um usuário

- **Login**

É a identificação do usuário para o Aker Configuration Manager. Não podem existir dois usuários com o mesmo login. Este login será pedido ao administrador do Aker Configuration Manager quando este for estabelecer uma sessão de administração remota.

O login deve ter entre 1 e 14 caracteres. Não há diferenças entre letras maiúsculas e minúsculas neste campo.

- **Nome**

Este campo contém o nome completo do usuário associado ao login. Os seu objetivo é de informação, não sendo usado para qualquer validação.

Este nome deve ser um conjunto de caracteres de comprimento entre 0 e 40.

- **Senha**

Este campo será usado em conjunto com o campo login para identificar um usuário perante o Aker Configuration Manager. Ao digitar a senha, serão mostrados na tela asteriscos "*" ao invés das letras.

O campo senha deve ter no máximo 14 caracteres. Neste campo, letras maiúsculas e minúsculas são consideradas diferentes.

É extremamente importante que as senhas usadas tenham um comprimento grande, o mais próximo possível do limite de 14 caracteres. Além disso, deve-se sempre utilizar uma combinação de letras minúsculas, maiúsculas, números e caracteres especiais nas senhas (caracteres especiais são aqueles encontrados no teclado dos computadores e que não são números nem letras: "$", "&",”]", etc). Nunca use como senhas palavras em qualquer idioma ou apenas números.

- **Confirmação**

Este campo serve para confirmar a senha digitada no campo anterior, uma vez que esta aparece como asteriscos.

- **Permissões do Firewall**

Este campo define o que um usuário pode fazer dentro do Firewall gerenciado pelo Aker Configuration Manager.

- **Permissões do Configuration Manager**

Este campo define o que um usuário pode fazer dentro do Aker Configuration Manager.

O objetivo destas permissões é possibilitar a criação de uma administração descentralizada para o Firewall. É possível, por exemplo, numa empresa que possua vários departamentos e vários Firewalls, deixar um administrador responsável pela configuração de cada um dos produtos e um responsável central com a tarefa de supervisionar a administração. Este supervisor seria a única pessoa capaz de apagar e alterar a configuração de log e eventos dos Firewalls. Desta forma, apesar de cada departamento ter autonomia de administração é possível ter um controle central do que cada administrador alterou na configuração e quando ele realizou cada alteração. Isto é um recurso muito importante para realizar auditorias internas, além de aumentar a segurança da administração.

Essas permissões consistem de três opções que podem ser marcadas independentemente.

Caso um usuário não possua nenhum atributo de autoridade, então, esse terá permissão apenas para visualizar a configuração do Aker Configuration Manager e compactar os arquivos de log e de eventos.

- **Configurando o Firewall e o Configuration Manager**

Em ambos os casos, se esta permissão estiver marcada, o usuário em questão poderá administrar o Aker Firewall ou o Aker Configuration Manager, isto é, alterar a configuração das entidades, regras de filtragem, conversão de endereços, criptografia, proxies e parâmetros de configuração que não estejam relacionados ao log.

- **Configurar Log**

Se esta opção estiver marcada, em ambos os casos, o usuário em questão terá poderes para alterar os parâmetros relacionados ao log (como por exemplo, tempo de permanência do log), alterar a configuração da janela de ações (tanto as mensagens quanto os parâmetros) e apagar permanentemente o log e os eventos.

- **Administrar Usuários**

Se esta opção estiver marcada, tanto no Firewall como no Configuration Manager, o usuário em questão terá acesso à janela de administração de usuários, podendo incluir, editar e excluir outros usuários.

Um usuário que possuir esta autoridade somente poderá criar, editar ou excluir usuários com autoridades iguais ou menores às que ele possuir (por exemplo, se um usuário tiver poderes de gerenciar usuários e configurar log, então ele poderá criar usuários que não possuam nenhuma autoridade, que somente possam configurar o log, que somente possam criar novos usuários ou que possam gerenciar usuários e configurar log. Ele não poderá nunca criar, nem editar ou excluir, um usuário que possa configurar o Firewall).

Aba Autenticação X509

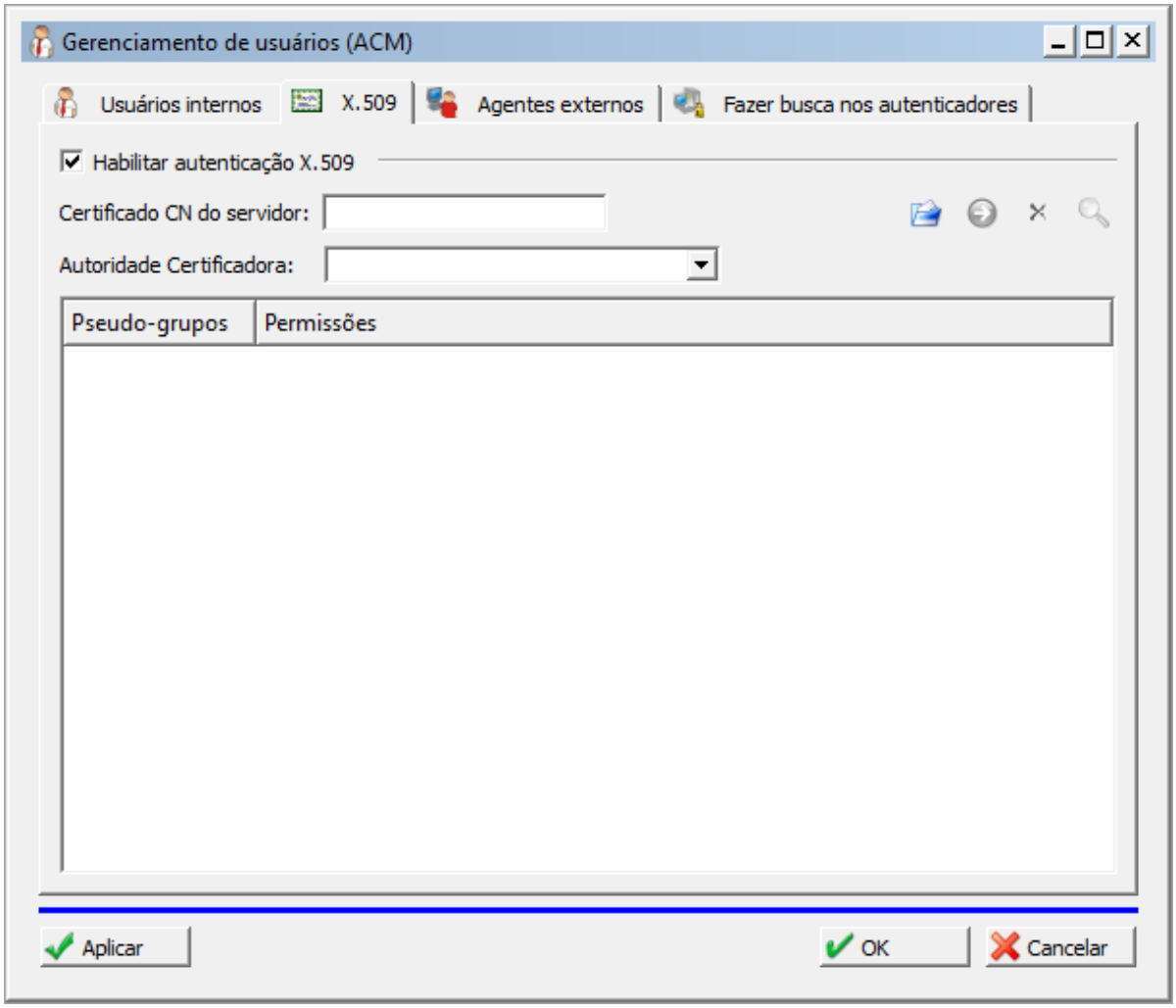

Figura 54 – Aba X.509

Essa aba consiste no método de autenticação com certificação digital X509. O Certificado Digital pode ser considerado como a versão eletrônica (digital) de uma cédula de identidade. Ele associa uma chave pública com a identidade real de um indivíduo, de um servidor, ou de alguma outra entidade. Um certificado digital, normalmente é usado para ligar uma entidade a uma chave pública. Para garantir a integridade das informações contidas neste arquivo, ele é assinado digitalmente, no caso de uma Infraestrutura de Chaves Públicas (ICP), o certificado é assinado pela Autoridade Certificadora (AC) que o emitiu e no caso de um modelo de Teia de Confiança (Web of trust) como o PGP, o certificado é assinado pela própria entidade e assinado por outros que dizem confiar naquela entidade. Em ambos os casos, as assinaturas contidas em um certificado são atestamentos feitos por uma entidade que diz confiar nos dados contidos naquele certificado.

Um certificado normalmente inclui:

Informações referentes à entidade para o qual o certificado foi emitido (nome, e-mail, CPF/CNPJ, PIS etc.)

- A chave pública referente à chave privada de posse da entidade especificada no certificado
- O período de validade
- A localização do "centro de revogação" (uma URL para download da CRL, ou local para uma consulta OCSP

A(s) assinatura(s) da(s) AC/entidade(s) que afirma que a chave pública contida naquele certificado confere com as informações contidas no mesmo

Um certificado padrão X.509 é outro formato de certificado muito comum. Todos os certificados X.509 obedecem ao padrão internacional ITU-T X.509; assim (teoricamente) certificados X.509 criados para uma aplicação podem ser usados por qualquer aplicação que obedece X.509.

Um certificado exige alguém para validar que uma chave pública e o nome do dono da chave vão juntos. Com certificados de PGP, qualquer um pode representar o papel de validador. Com certificados X.509, o validador é sempre uma Autoridade de Certificação ou alguém designado por uma CA.

Um certificado X.509 é uma coleção de um conjunto padrão de campos contendo informações sobre um usuário ou dispositivo e sua correspondente chave pública. O padrão X.509 define qual informação vai no certificado, e descreve como codificar isto (o formato dos dados). Todos os certificados X.509 têm os seguintes dados:

- O número da versão do X.509 que identifica qual o padrão será aplicado na versão do X.509 para este certificado, o que afeta e qual informação pode ser especificada neste.
- A chave pública do possuidor do certificado junto com um algoritmo de identificação, especifica qual sistema de criptografia pertence à chave e quaisquer parâmetros associados.

Abaixo, seguem os campos que contém a aba X.509:

- **Habilitar autenticação X.509**: Ao selecionar essa opção permite habilitar a autenticação do usuário via certificado digital x.509.
- **CN do Certificado do Firewall**: Essa opção mostra qual certificado o Aker Configuration Manager está utilizando para a autenticação.

Importa Certificado: Ao clicar nesse ícone, permite a inclusão de um novo certificado, ou seja, carrega-se o certificado cadastrado no arquivo, incluindo-o no Aker Configuration Manager.

- **Exporta Certificado**: Gravam os dados do certificado, para transportá-lo para uma futura aplicação desse certificado. Tira uma cópia do certificado.
- **Remove Certificado**: Ao clicar nesse ícone, permite a remoção do certificado que foi incluído. Com isso o Aker Configuration Manager fica sem nenhum certificado.

- **Visualiza detalhes dos certificados**: Mostra todas as informações contidas no certificado habilitado.
- **Autoridade Certificadora**: A autoridade certificadora *(CA- certificate authority)* deve garantir ao usuário, através da assinatura de seus certificados, que tais entidades são realmente quem dizem ser. Então, a CA tem um papel básico de garantir a correspondência entre a identidade e a chave pública de uma determinada entidade, sabendo que tal chave pública corresponde a uma chave privada que permanece sob guarda exclusiva dessa entidade.

Para tanto, a CA deve ser capaz de realizar todos os processos de emissão de certificados, verificação de validade, armazenamento, publicação ou acesso on-line, revogação e arquivamento para verificação futura.

Essa opção permite selecionar uma autoridade a qual o usuário está vinculado.

Em consequência, uma autoridade certificadora constitui-se de um sistema computacional completo, com capacidade de comunicação processamento e armazenamento. Além disso, tanto as comunicações envolvendo esse sistema, assim como o próprio sistema, devem ser também protegidos e a própria identidade do sistema deve ser garantida, necessidades estas que são atendidas por intermédio da publicação de uma chave pública pertencente à própria autoridade certificadora. Como tal chave deve também ser garantida com um certificado digital, então, em geral, uma autoridade certificadora deposita sua chave pública junto a outra autoridade certificadora, formando uma estrutura de certificação onde algumas CAs funcionam como autoridades certificadoras para outras CAs.

- **Pseudo-Grupos**: Corresponde aos grupos de certificados relacionados à autoridade certificadora selecionada na opção acima. Este campo não é editável.
- **Permissões**: Esse campo das permissões é editável, podendo, para cada CA selecionada, relacionar as permissões para cada grupo.

Nessa opção, uma vez escolhida uma Autoridade Certificadora e definidos os níveis/permissões de acesso para cada grupo, ao trocar de CA todas as permissões relacionadas a outra CA serão perdidas.

Aba Agentes Externos

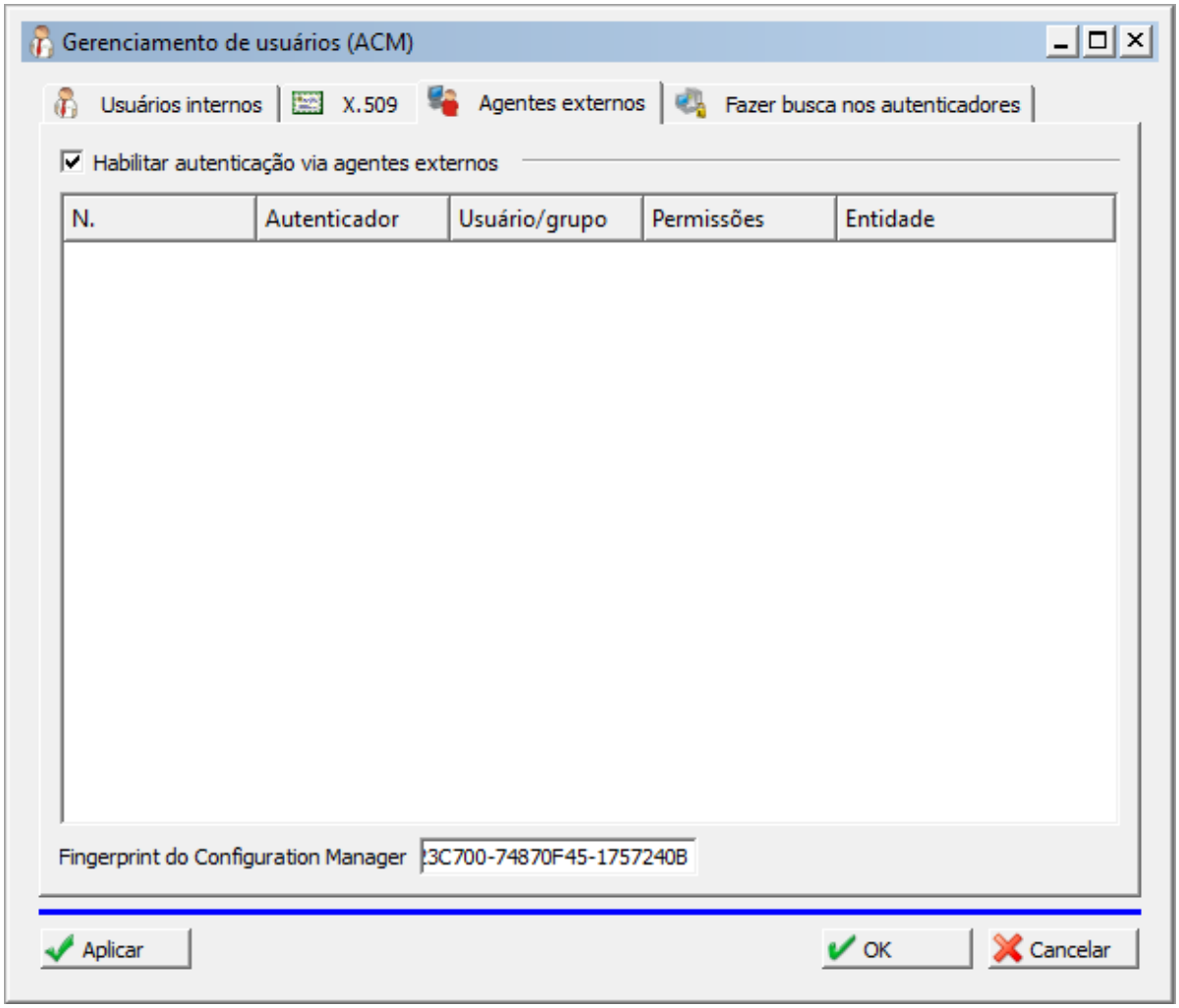

Figura 55 – Aba Agentes externos

Esta aba consiste na configuração dos agentes externos que serão utilizados para a autenticação dos usuários que administram o Aker Configuration Manager, definindo assim regras de autenticação para o acesso destes.

Habilita a autenticação por agentes externos

Ao selecionar essa opção permite a autenticação dos usuários, por meio dos agentes externos que estão cadastrados no Aker Configuration Manager. Permite definir qual usuário/grupo presente nesse autenticador, quais as permissões de acesso desse usuário/grupo, e a definição das entidades que o usuário utilizará para conectar ao Aker Configuration Manager.

Autenticador

Ao clicar com o botão direito na coluna autenticador, será possível selecionar um autenticador (agente externo) previamente listado na aba autenticadores dessa mesma

janela. Esse autenticador será responsável por intermediar o processo de autenticação da interface com o Aker Configuration Manager.

Usuário/Grupo

Nessa coluna, deve-se selecionar os usuários ou grupos relacionados ao autenticador escolhido. Pode-se associar um usuário somente ou um grupo deles.

Permissões

Este campo define o que um usuário pode fazer dentro do Aker Firewall. Ele consiste de seis opções que podem ser marcadas independentemente.

O objetivo destas permissões é possibilitar a criação de uma administração descentralizada para o Aker Configuration Manager. É possível por exemplo, numa empresa que possua vários departamentos e vários Aker Configuration Manager, deixar um administrador responsável pela configuração de cada um dos Aker Configuration Manager e um responsável central com a tarefa de supervisionar a administração. Este supervisor seria a única pessoa capaz de apagar e alterar a configuração de log e eventos dos Aker Configuration Manager. Desta forma, apesar de cada departamento ter autonomia de administração é possível ter um controle central do que cada administrador alterou na configuração e quando ele realizou cada alteração. Isto é um recurso muito importante para realizar auditorias internas, além de aumentar a segurança da administração.

Entidades

Essa opção permite definir de qual entidade o usuário se conectará ao Aker Configuration Manager. Este campo é opcional.

Configuration Manager Fingerprint

É um resumo da identificação do certificado digital do Aker Configuration Manager. Essa opção possibilita ao usuário identificar quando há uma mudança no Configuration Manager associado, permitindo identificar eventuais fraudes.

Aba Fazer busca nos autenticadores

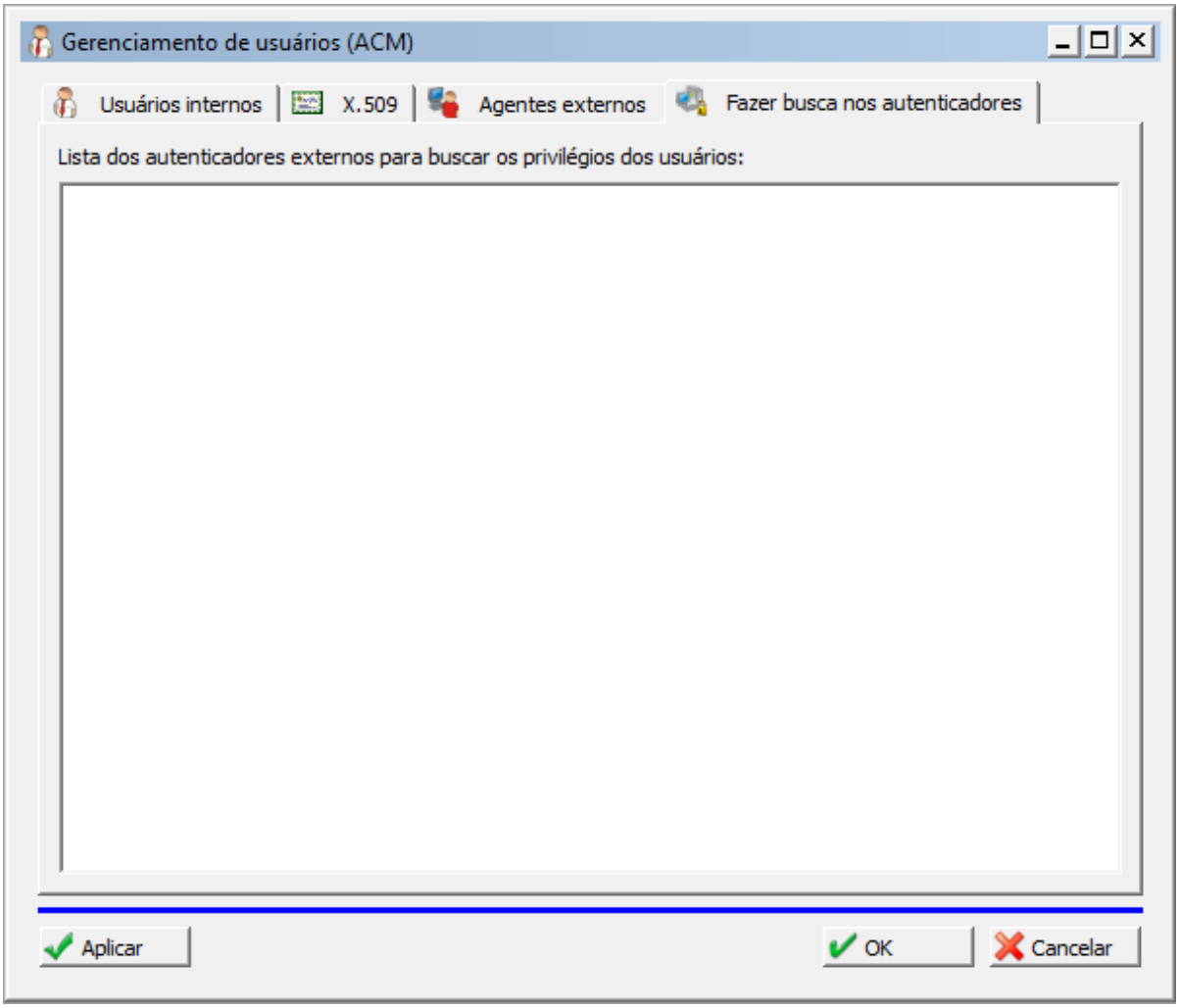

Figura 56 – Aba Fazer busca nos autenticadores

Esta aba permite listar os autenticadores cadastrados que serão inseridos na aba Agentes externos do Configuration Manager. Para realizar qualquer alteração nesta aba é necessário que ela esteja habilitada, para isso, deve-se clicar na opção "Habilita a autenticação por agentes externos" localizada na aba Agentes externos. Feito isto, ela estará habilitada para se fazer as alterações desejadas.

Lista de autenticadores externos para a pesquisa dos privilégios dos usuários: Este campo permite listar as entidades que serão inseridas na coluna autenticadores da aba Agentes externos, as quais serão gerados os usuários/grupos dessa aba. Para este procedimento deve-se clicar com o botão esquerdo dentro da coluna da aba Autenticadores a pesquisar,

adicionar entidades, Autenticador1, em seguida clicar no botão OK da aba Agentes externos para que seja efetuada essa operação.

Ao realizar esta operação é necessário que as entidades já estejam previamente cadastradas. Para maiores informações sobre como configurar essas entidades, basta consultar o capítulo intitulado "Cadastrando Entidades" que está disposto neste manual.

É através dessa aba que se aplicam as configurações das entidades que serão listadas na Aba Agentes externos. Para listar os usuários/grupos na Aba Agentes externos, será necessário antes aplicar as configurações dessa janela.

É possível criar usuários diretamente no servidor onde o Aker Configuration Manager está rodando, basta entrar no diretório de instalação (/usr/local/aker/centralizador) e digitar o comando **./aker_conf_manager-adduser <usuario> <senha>** onde <usuario> representa o login do usuário que está sendo adicionado e <senha> representa sua permissão. Isso permite a criação de usuários quando a autenticação pela Interface Remota não está disponível.

Ao se realizar quaisquer alterações de configuração no Configuration Manager ou em um dos Firewalls que ele gerencia, deve-se salvar essas alterações clicando no ícone "*Efetuar mudanças*" ( ) que é localizado na parte superior da Control Center, para que as modificações efetuadas sejam de fato salvas.

Configuração de parâmetros

7 Configuração de parâmetros

Neste capítulo serão mostrados quais são e como devem ser configurados os parâmetros essenciais para que seja possível a conexão de usuários ao Aker Configuration Manager pelo Aker Control Center.

O que são os parâmetros?

Esses parâmetros servem para informar a partir de quais endereços e portas o Aker Configuration Manager está sendo executado. Os tempos de expiração por inatividade de cada conexão e para definir uma lista de controle de acesso.

7.1 Configurando os Parâmetros

Essa janela consiste de duas partes distintas: a primeira aba corresponde a Parâmetros Globais onde os usuários e grupos de autenticadores são associados com perfis de acesso. A configuração desta aba será vista em detalhes em Perfis de Acesso de Usuários, na segunda aba escolhe-se os Métodos de autenticação onde se determina os parâmetros relativos à autenticação de usuários por meio de nomes/senhas e se configuram os parâmetros de autenticação por token (SecurID) e Autoridade Certificadora (PKI). Na segunda aba é configurado o Controle de Acesso por IP que também será visto com mais detalhes em Perfis de Acesso de Usuários.

- O botão **OK** fará com que a janela de configuração de parâmetros seja fechada e as alterações feitas sejam salvas
- O botão **Cancelar** fará com que a janela seja fechada, porém as alterações efetuadas não sejam aplicadas.
- O botão **Aplicar** fará com que as alterações feitas sejam salvas e manterá a janela aberta.

Para ter acesso a janela de parâmetros de autenticação siga os passos a seguir:

Figura 57 – Configurações: Parâmetros

- Clicar no menu *Configurações*
- Selecionar a opção "*Parâmetros*"

Aba Parâmetros globais

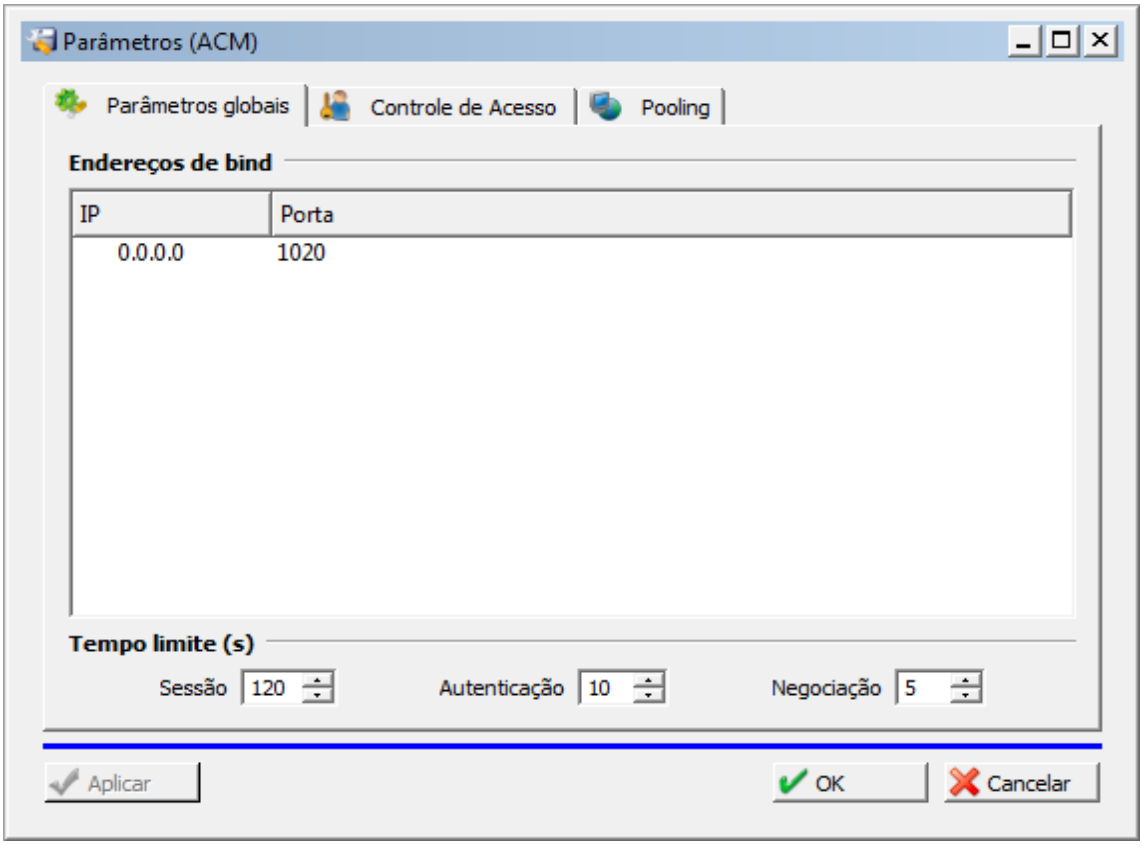

Figura 58 – Aba Parâmetros globais

- **Endereços de bind**: Este campo permite adicionar os IPs e as portas a partir das quais o Aker Configuration Manager poderá ser encontrado na rede, ou seja, conectar ao CM através desses endereços.

Os IPs fornecidos nessa janela devem estar presentes nas configurações das interfaces de rede do servidor onde o CM está rodando.

Os IPs fornecidos restringem a conexão apenas a eles, ou seja, se o servidor possuir dois endereços de rede, mas apenas um deles é configurado nessa janela, somente esse que foi configurado poderá ser utilizado. Caso o administrador não deseje restringir o IP de conexão, basta incluir o IP 0.0.0.0 e a porta de preferência, ou optar pela porta padrão 1020.

É preciso garantir que o endereço IP informado pertença ao conjunto dos endereços associados à máquina do CM, caso contrário haverá uma impossibilidade de conexão. O usuário não conseguirá conectar, se isso ocorrer, é necessário entrar em contato com o Suporte Técnico da Aker.

- **Tempo limite (s)**: Define o tempo máximo para uma conexão expirar por inatividade. São valores diferentes para Sessão, Autenticação e Negociação da autenticação.
- **Sessão**: Define o tempo decorrido depois que o usuário já está conectado e autenticado, ou seja, quando ele já tem acesso ao produto e pode configurá-lo.
- **Autenticação**: Define o tempo gasto para ser autenticado.
- **Negociação**: É o tempo (tempo máximo, na autenticação) gasto para negociar o tipo de autenticação (definir se será por usuário/senha, X.509, agentes externos etc.).
- **Log**: Permite adicionar os logs do CM aos logs do sistema.

Aba Controle de Acesso

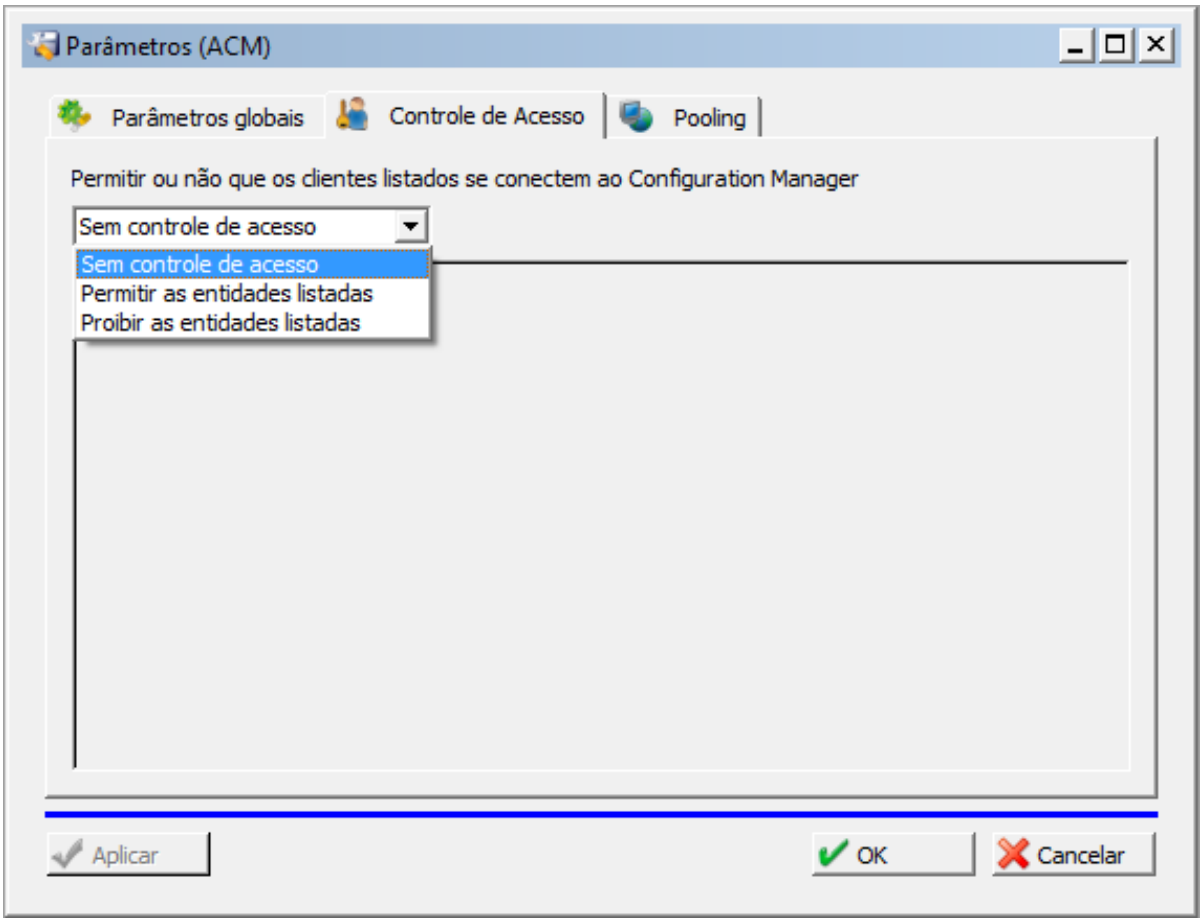

Figura 59 – Aba Controle de Acesso

Esta aba permite controlar o acesso pelo endereço IP de origem de quem deseja gerenciar o Configuration Manager. O endereço do Control Center que irá se conectar no CM deve atender a esse controle. São eles:

- **Sem Controle de acesso**: sem restrições, de qualquer lugar pode-se conectar no CM.
- **Permitir as entidades listadas**: apenas os endereços de origem representados por essas entidades poderão se conectar.
- **Proibir entidades listadas**: Apenas esses endereços estarão proibidos, e os outros liberados.

Aba Pooling

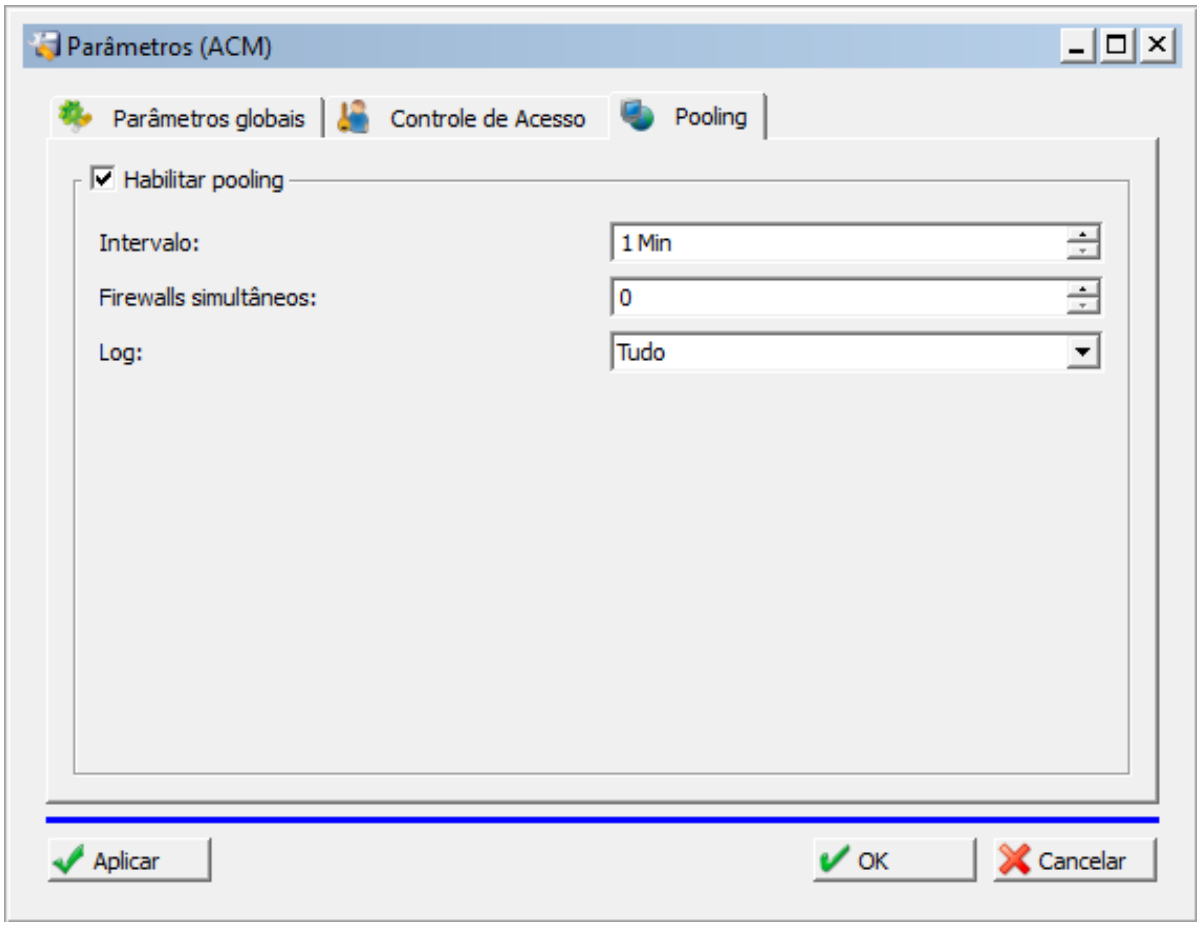

Figura 60 – Aba Pooling

Esta Janela possibilita ao usuário verificar as configurações dos firewalls que estão sendo gerenciados no Aker Configuration Manager.

Habilitar pooling: Habilita a verifcação de configuração dos firewalls que estão sendo gerenciados pelo Aker Configuration Manager.

- **Intervalo**: Esta opção define o intervalo que a verificação será efetuada em minutos.
- **Firewalls simultâneos:** Define o numero de Firewalls que serão verificados simultâneamente.
- **Log:** Esta opção define se o log de verificação será feito apenas sobre os erros, ou todas a ações efetuadas no Firewall.

Ao se realizar quaisquer alterações de configuração no Configuration Manager ou em um dos Firewalls que ele gerencia, deve-se salvar essas alterações clicando no ícone "*Efetuar mudanças*" ( ) que é localizado na parte superior da Control Center, para que as modificações efetuadas sejam de fato salvas.

Cadastrando Entidades

8 Cadastrando Entidades

Será mostrado neste capítulo o que são, para que servem e como cadastrar entidades no Aker Configuration Manager.

O que são e para que servem as entidades?

Entidades são representações de objetos do mundo real para o Aker Configuration Manager. Através delas, podem-se representar máquinas, redes, serviços a serem disponibilizados, entre outros.

A principal vantagem da utilização de entidades para representar objetos reais é que a partir do momento em que são definidas no Configuration Manager, elas podem ser referenciadas como se fossem os próprios objetos, propiciando uma maior facilidade de configuração e operação. Todas as alterações feitas em uma entidade serão automaticamente propagadas para todos os locais onde ela é referenciada.

Pode-se definir, por exemplo, uma máquina chamada de Servidor WWW, com o endereço IP de 10.0.0.1. A partir deste momento, não é mais necessário se preocupar com este endereço IP. Em qualquer ponto onde seja necessário referenciar esta máquina, a referência será feita pelo nome. Caso futuramente seja necessário alterar seu endereço IP, basta alterar a definição da própria entidade que o sistema automaticamente propagará esta alteração para todas as suas referências.

O Configuration Manager lida com três tipos de entidades. São elas:

Entidades Locais: Essas entidades são as que podem ser estabelecidas individualmente para cada Firewall, por meio da interface do Configuration Manager, que acessa diretamente cada Firewall gerenciado.

Entidades Globais: Essas entidades são como as entidades locais do Firewall, mas elas só podem ser criadas e apagadas pelo Configuration Manager.

Entidades Globais Dependentes: Essas entidades possuem valor variável em cada Firewall gerenciado.

Existem três tipos possíveis de entidades globais dependentes: Máquinas, Redes e Serviços.

Para maiores informações de como definir as entidades, basta consultar o capítulo intitulado "Cadastrando Entidades" do manual do Firewall.

8.1 Cadastrando entidades utilizando a Interface Remota

Para ter acesso à janela de cadastro de entidades deve-se:

- Clicar no menu Configurações do Aker Configuration Manager que se quer administrar;
- Pressione a tecla F5 (a janela será mostrada abaixo da janela com os menus de configuração do Aker Configuration Manager).

A janela Entidades

Essa janela é composta por duas abas: Genéricas e Grupos.

Aba Genéricas

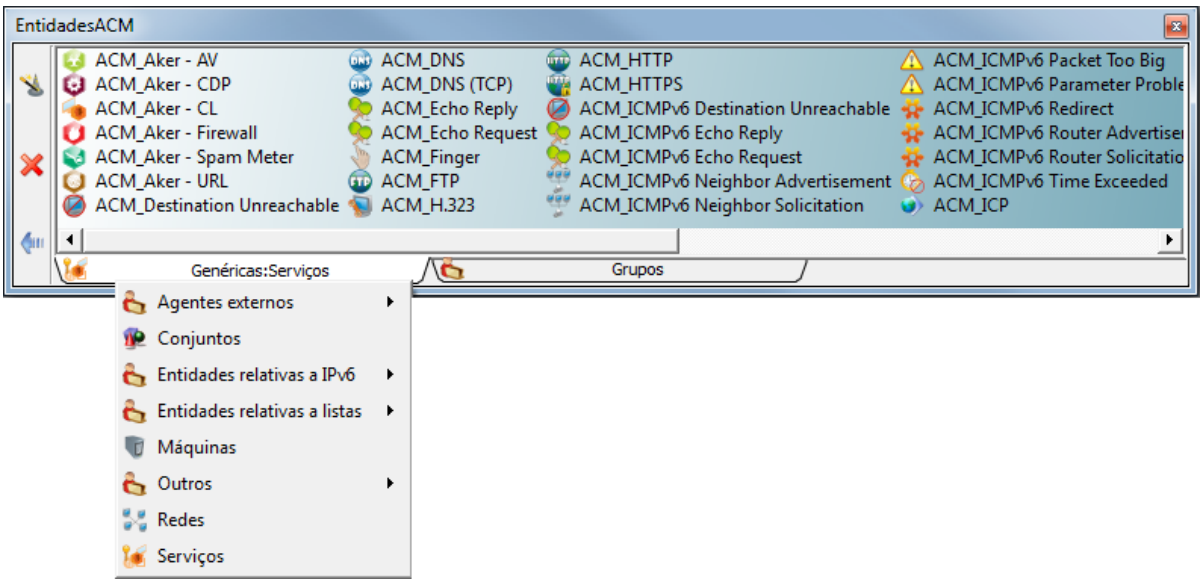

Figura 61 – Aba genéricas

A janela de cadastro de entidades é onde são cadastradas todas as entidades do Aker Configuration Manager, independente do seu tipo. Esta janela, por ser constantemente utilizada em praticamente todas as demais configurações do Aker Configuration Manager, normalmente é mostrada sempre aberta na horizontal, abaixo da janela com os menus de configuração de cada Aker Configuration Manager.

Aba Grupos

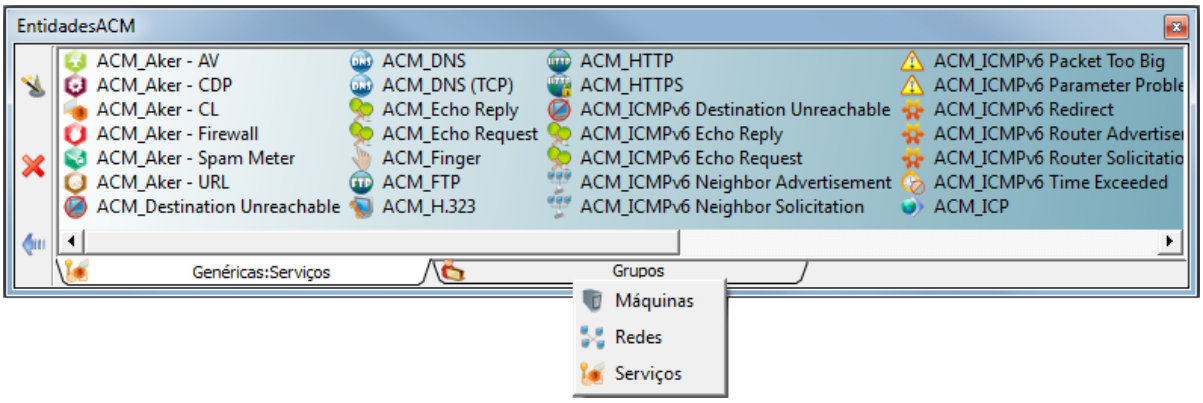

Figura 62 – Aba Grupos

Esta janela permite criar entidades que sofrem uma interpretação diferente em cada Firewall gerenciado.

Dica: É possível posicionar a janela de entidades como se fosse uma janela comum, bastando para isso Clicar sobre sua barra de título e arrastá-la para a posição desejada.

Dica: Para criar uma nova entidade, caso a lista de entidades criadas esteja cheia, deve-se clicar em cima da aba que fica na parte inferior da janela.

Nesta janela estão desenhados oito ícones, em forma de árvore, que representam os oito tipos de entidades possíveis de serem criados.

Dica: Para visualizar as entidades criadas simplesmente Clicar no sinal de '+' e as entidades ficarão listadas logo abaixo do logotipo, ou clicar sobre a aba correspondente a entidade que se deseja visualizar.

Para cadastrar uma nova entidade, deve-se proceder da seguinte forma:

1. Clicar uma vez no ícone correspondente à entidade do tipo que deseja criar com o botão direito do mouse e selecionar a opção Inserir no menu pop-up

Ou

2. Clicar no ícone correspondente à entidade do tipo que deseja criar e pressionar a tecla *Insert*.

Para editar ou excluir uma entidade, deve-se proceder da seguinte forma:

- Selecionar a entidade a ser editada ou excluída (se necessário, expande-se a lista do tipo de entidade correspondente)

Clicar com o botão direito do mouse e selecionar a opção **Editar** ou **Apagar**, respectivamente, no menu pop-up que aparecer.

Ou

- Clicar no ícone correspondente à entidade do tipo que deseja criar e pressionar a tecla *Delete*.

No caso das opções **Editar** ou **Incluir**, aparecerá a janela de edição de parâmetros da entidade a ser editada ou incluída. Esta janela será diferente para cada um dos tipos possíveis de entidades.

O ícone ( ) localizado a esquerda da janela aciona o assistente de cadastramento de entidades que será descrito no final deste capítulo.

Para se obter maiores informações de como Incluir/editar entidades, basta consultar o capítulo ***"Cadastrando Entidades"*** do manual do Firewall.

Incluindo / editando máquinas (Entidades Grupos)

Essas entidades possuem valor variável em cada Firewall gerenciado.

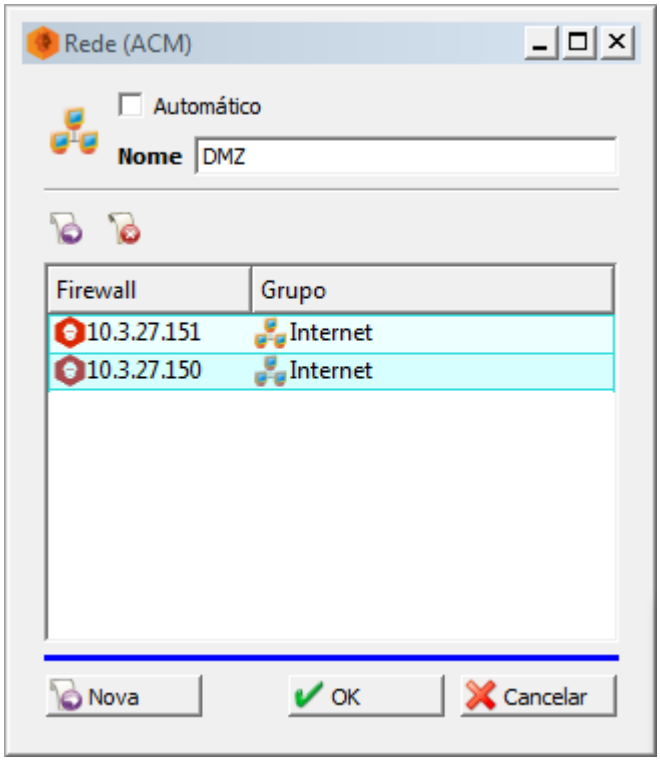

Figura 63 – Incluindo /editando máquinas

Essa janela permite definir entidades com um significado diferente em cada Firewall. Na coluna "Firewall", é permitido especificar cada Firewall gerenciado associando-o com uma de suas entidades na coluna "Grupo".

É possível definir uma rede, exemplo: DMZ, em que no FW01 será DMZ Suporte, e corresponda a 10.1.0.0, e no FW02 significa DMZ Homologação e corresponda a 10.2.0.0 em outro FW03 significa DMZ Desenvolvimento e corresponda a 10.3.0.0.

Desta forma, as regras criadas no Configuration Manager que utilizem "DMZ", e que sejam aplicadas em certo Firewall, serão traduzidas automaticamente na rede apropriada de cada Firewall, de acordo com a associação feita na configuração das entidades dependentes.

Ao se realizar quaisquer alterações de configuração no Configuration Manager ou em um dos Firewalls que ele gerencia, deve-se salvar essas alterações clicando no ícone "*Efetuar mudanças*" ( ) que é localizado na parte superior da Control Center, para que as modificações efetuadas sejam de fato salvas.

O Filtro de Estados

9 O Filtro de Estados

Este capítulo mostra como configurar as regras que propiciarão a aceitação ou não de conexões pelo Aker Configuration Manager. Este módulo é o mais importante do sistema e é onde normalmente se gasta o maior tempo de configuração.

Planejando a instalação

Para maiores informações, do que é um filtro de pacotes e como montar regras de filtragem em um filtro de pacotes simples, basta consultar o capítulo intitulado "O Filtro de Estados" do manual do Firewall.

Montando regras de filtragem no Aker Configuration Manager para os Firewalls gerenciados

Configurar as regras de filtragens no Aker Configuration Manager é algo muito fácil em função de sua concepção inteligente. Toda a parte de endereços IP, máscaras, protocolos, portas são interfaces e são configuradas nas entidades (para maiores informações, veja o capítulo intitulado Cadastrando Entidades). Com isso, ao configurar uma regra não é necessário preocupar com qual porta um determinado serviço utiliza ou qual o endereço IP de uma rede. Tudo isso já foi previamente cadastrado. Para facilitar ainda mais, todos os serviços mais utilizados na Internet já vem previamente configurados de fábrica, não havendo a necessidade de gastar tempo pesquisando os dados de cada um.

Basicamente, para cadastrar uma regra, o administrador deve especificar as entidades de origem, destino e os serviços que farão parte da regra. Ele pode também especificar uma interface de origem para os pacotes e definir em quais horários a regra estará ativa, em uma tabela de horários semanal. Com o uso desta tabela de horários é possível liberar determinados serviços em determinadas horas do dia (por exemplo, liberar IRC, ou bate-papo, apenas nos horários fora do expediente). Se um pacote chegar em um horário no qual a regra não está marcada como ativa, ela será ignorada, fazendo com que a busca continue na próxima regra da lista.

O funcionamento do filtro é simples: o firewall irá pesquisar uma a uma as regras definidas pelo administrador, na ordem especificada, até que o pacote se encaixe em uma delas. A partir deste momento, ele irá executar a ação associada à regra, que pode ser aceita, rejeitada ou descartada (estes valores serão explicados no próximo tópico). Caso a pesquisa chegue ao final da lista e o pacote não se enquadre em nenhuma regra, então, este será descartado (é possível configurar ações para serem executadas neste caso). Isto será tratado no capítulo intitulado: Configurando as ações do sistema.

9.1 Editando uma lista de regras usando a Interface Remota

Para ter acesso a janela de configuração de regras basta:

Figura 64 – Políticas: Regras de filtragem

- Clicar no menu *Políticas* da janela principal
- Selecionar a opção "*Regras de Filtragem*"

A janela de regras de filtragem

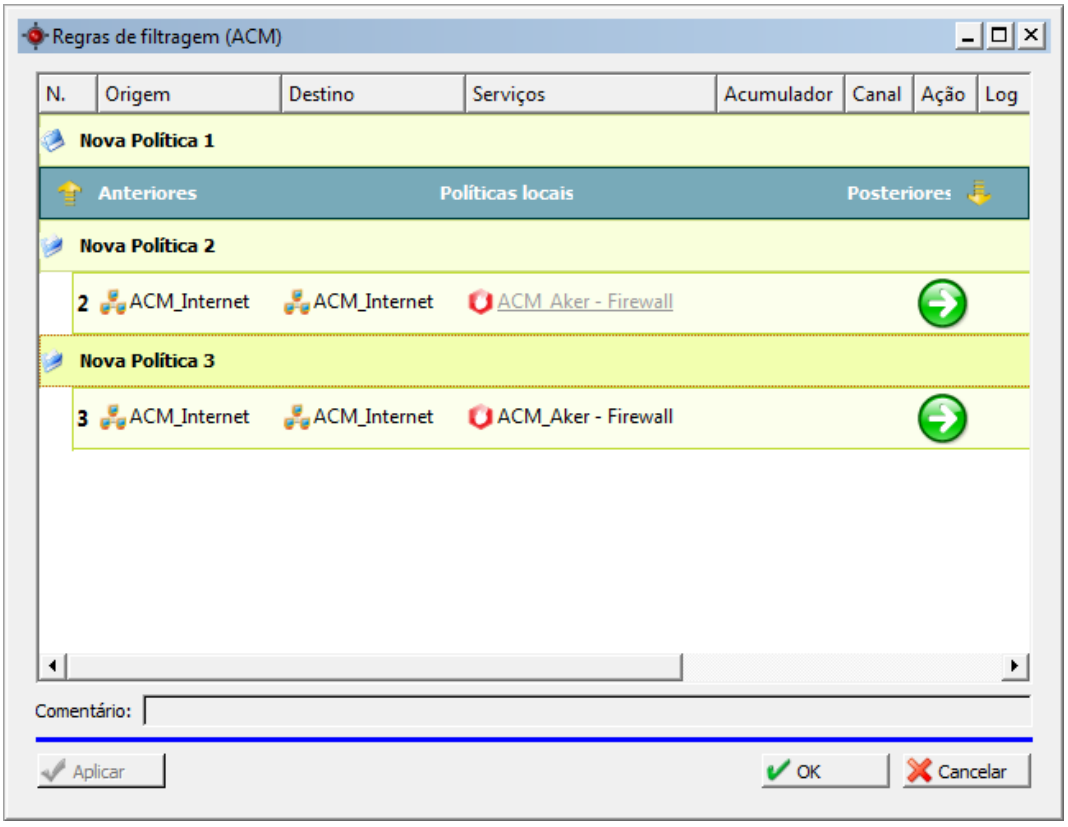

Figura 65 – Janela de Regras de filtragem

A janela de regras contém todas as regras de filtragem definidas no Aker Configuration Manager. Cada regra será mostrada em uma linha separada, composta de diversas células. Caso uma regra esteja selecionada, ela será mostrada em uma cor diferente.

- O botão **OK** fará com que o conjunto de regras seja atualizado no contexto do Configuration Manager.
- O Botão **Cancelar** fará com que todas as alterações feitas sejam desprezadas e a janela seja fechada.
- O botão **Aplicar** enviará para o Configuration Manager todas alterações feitas, porém manterá a janela aberta.

Caso alguma regra possua um comentário, este pode ser visualizado na parte inferior da janela selecionando a regra desejada

O Marcador de políticas locais serve para representar as políticas locais de cada firewall gerenciado pelo CM. Assim, é possível definir se as regras do CM se encontrarão antes ou depois das regras configuradas individualmente em cada firewall. Isso é importante porque, como descrito em parágrafo anterior, a ordem das regras interfere na forma em que um pacote é filtrado.

Ao se adicionar uma nova política, deve-se, então, definir se ela estará antes ou depois das regrais locais do firewall. Isso é possível definindo sua posição em relação à linha verde.

Para executar qualquer operação sobre uma determinada regra, deve-se clicar com o botão direito do mouse sobre o campo que queira alterar. Aparecerá um menu com as opções de entidades referentes ao campo, como na figura abaixo:

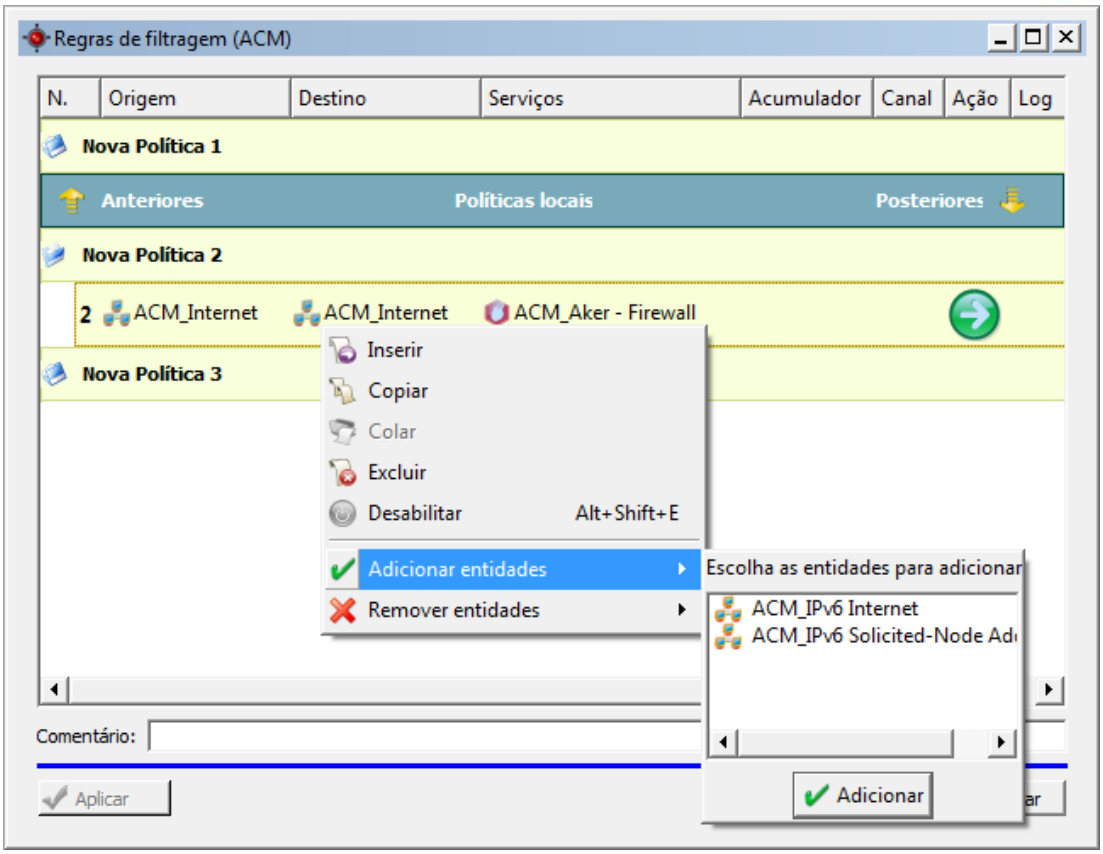

Figura 66 – Opções da Janela de regras de filtragem

- **Inserir**: Incluir uma nova regra na lista. Se alguma regra estiver selecionada, a nova regra será inserida na posição da selecionada. Caso contrário, a nova regra será incluída no final da lista.
- **Copiar**: Copiar a regra selecionada para uma área temporária.
- **Cola**r: Copiar a regra da área temporária para a lista. Se uma regra estiver selecionada, a nova será copiada para a posição da regra selecionada. Caso contrário ela será copiada para o final da lista.
- **Excluir**: Remover da lista a regra selecionada.
- **Habilitar/Desabilitar**: Desabilitar/habilitar a regra selecionada.
- **Adicionar entidades**: Adicionar uma entidade cadastrada no Configuration Manager. Veja se o ponteiro do mouse está sobre o campo o qual se quer inserir a entidade.
- **Remover entidades**: Remover uma entidade que foi inserida na regra.

Dica: A posição de cada regra pode ser alterada, bastando clicar e arrastar a mesma para a nova posição desejada, soltando-a em seguida.

Políticas: pode-se definir uma nova política, clicando no botão ( ) na barra de ferramentas do Configuration Manager. É possível editar um nome e uma cor para cada política, inclusive a padrão.

Para obter maiores informações de como construir as regras, consulte o capítulo intitulado "O Filtro de Estados" do manual do Firewall.

9.2 Associações

Para ter acesso a janela Associações deve-se:

Figura 67 – Políticas: Associações

- Clicar no menu *Políticas* da janela principal
- Selecionar a opção *"Associações"*

Aba Editar

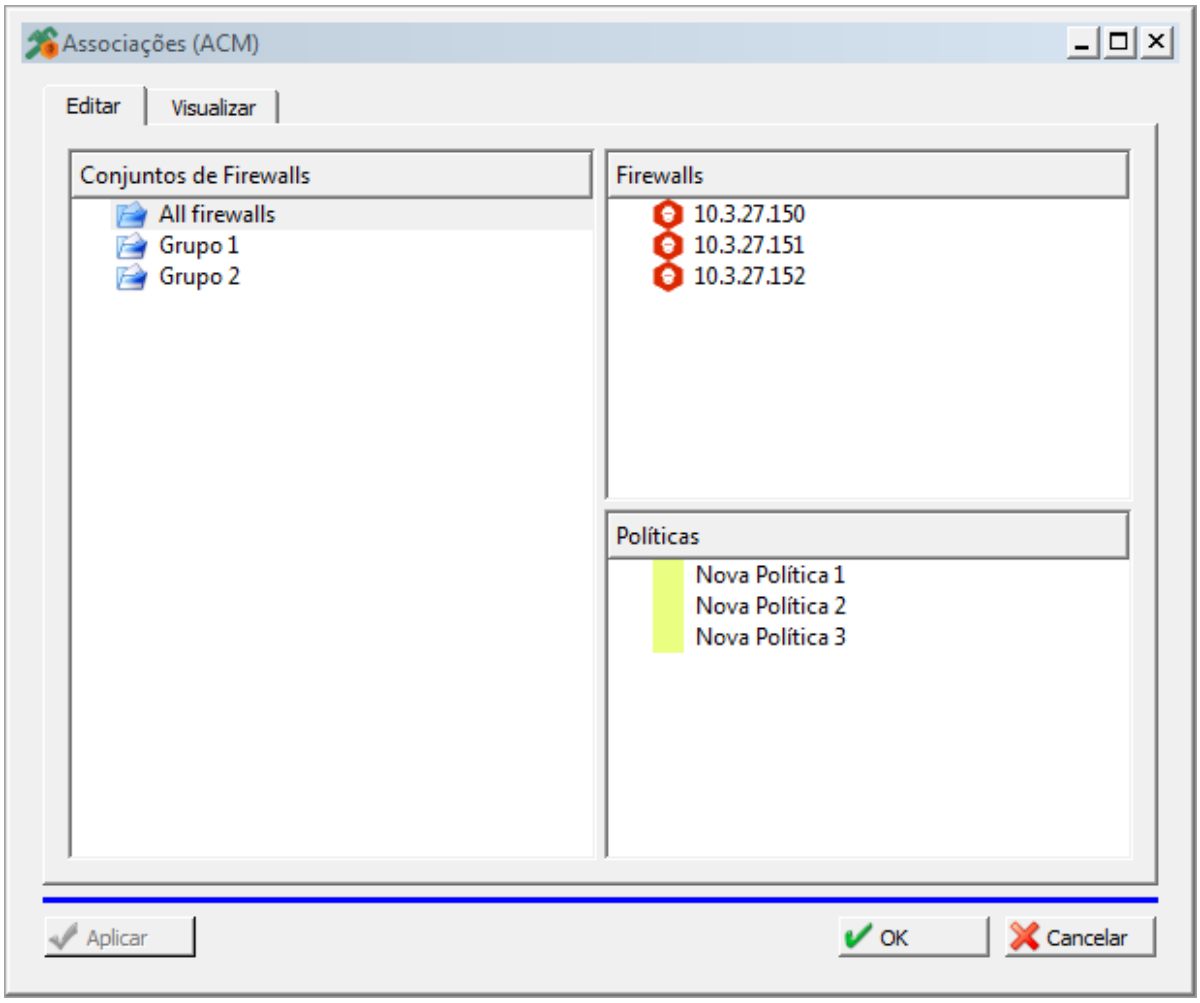

Figura 68 – Aba Editar

Esta aba permite definir grupos de Firewalls e as políticas que serão aplicadas a cada um desses grupos. Para inserir grupos, deve-se clicar com o botão esquerdo do mouse dentro da coluna Grupos e Selecionar a opção inserir.

- O botão **OK** fará com que as configurações aplicadas sejam salvas e a janela seja fechada.
- O Botão **Cancelar** fará com que todas as alterações feitas sejam desprezadas e a janela seja fechada.
- O botão **Aplicar** enviará para o Configuration Manager todas alterações feitas, porém manterá a janela aberta.

Ao selecionar um grupo na lista e clicar com o botão esquerdo, aparecerá a seguinte janela:

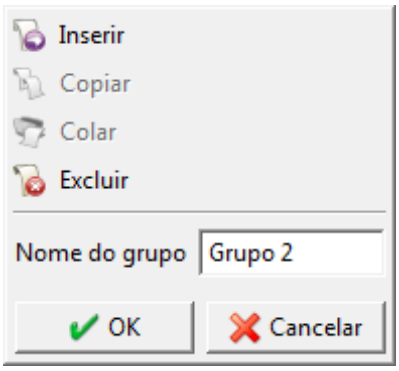

Figura 69 – Menu de opções

Inserir: permite inserir um novo grupo.

Excluir: remove o grupo de Firewalls selecionado.

Nome do grupo: Permite editar o nome do grupo selecionado.

Para adicionar um Firewall a um grupo, deve-se clicar no grupo em questão e, com o botão esquerdo do mouse dentro da coluna Firewalls, incluir o Firewall desejado, conforme demonstrado abaixo.

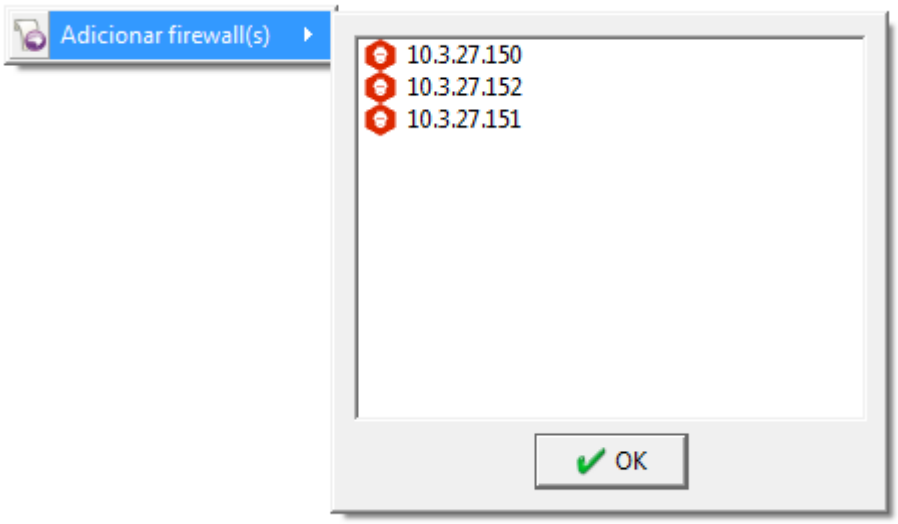

Figura 70 – Adicionando Firewalls

Os passos para se inserir as Políticas são os mesmos descritos no texto acima.

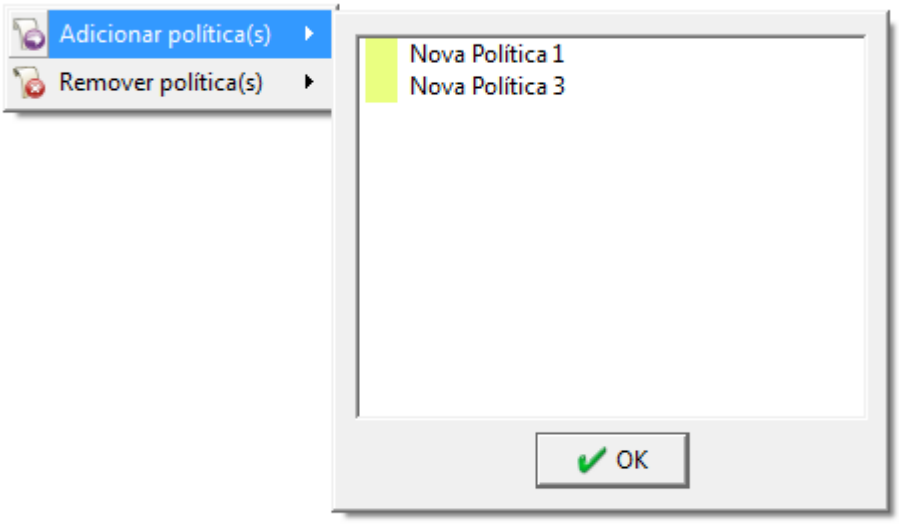

Figura 71 – Adicionando ou removendo Políticas

Sempre haverá um grupo padrão que inclui todos os Firewalls. No exemplo demonstrado abaixo, foram criados dois grupos extras, que contêm somente um Firewall cada. Esses grupos são chamados de Grupo 1 e Grupo 2. Veja as três figuras abaixo:

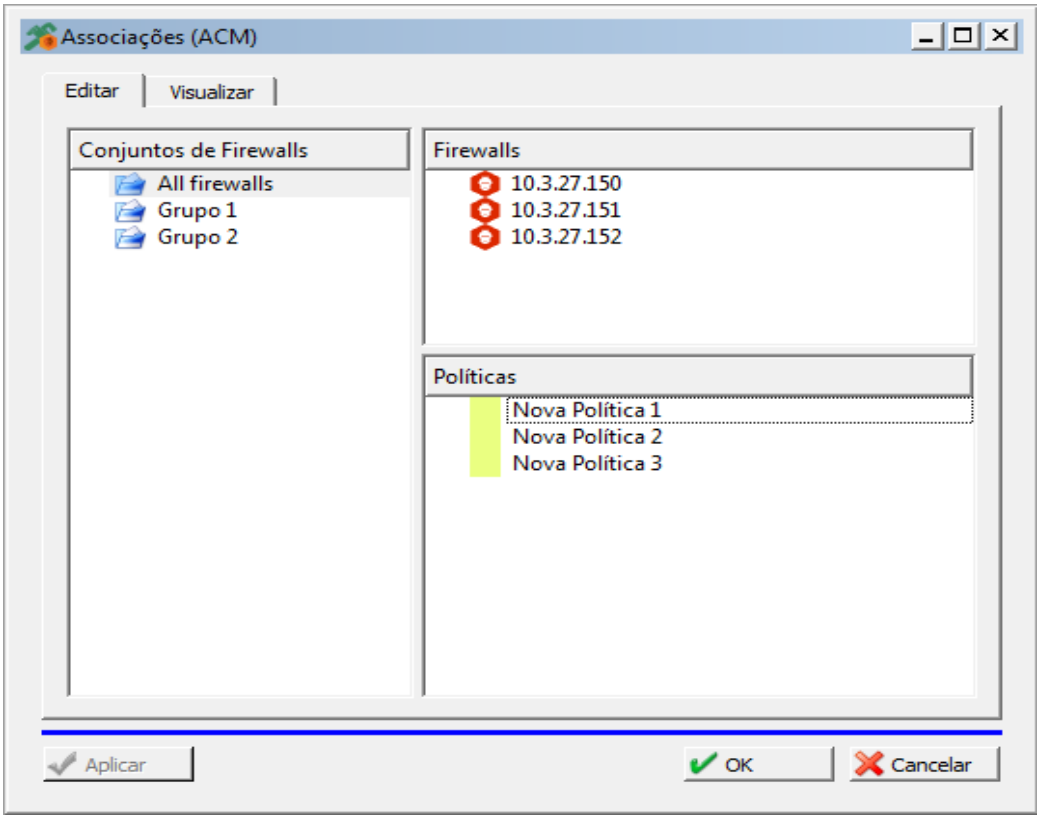

Figura 72 – Associações: Aba Editar

Aba Visualizar

Esta aba permite visualizar os grupos, os Firewalls, e as Políticas que foram configuradas. Para visualizá-los, deve-se clicar em um dos botões localizados na parte superior desta

janela. Esses botões são: Grupo, Firewall e Política. Depedendo do botão selecionado, as associações entre grupos, Firewalls e Políticas serão exibidas de uma determinada maneira, mas sempre mostrando hierarquicamente as relações entre esses conceitos.

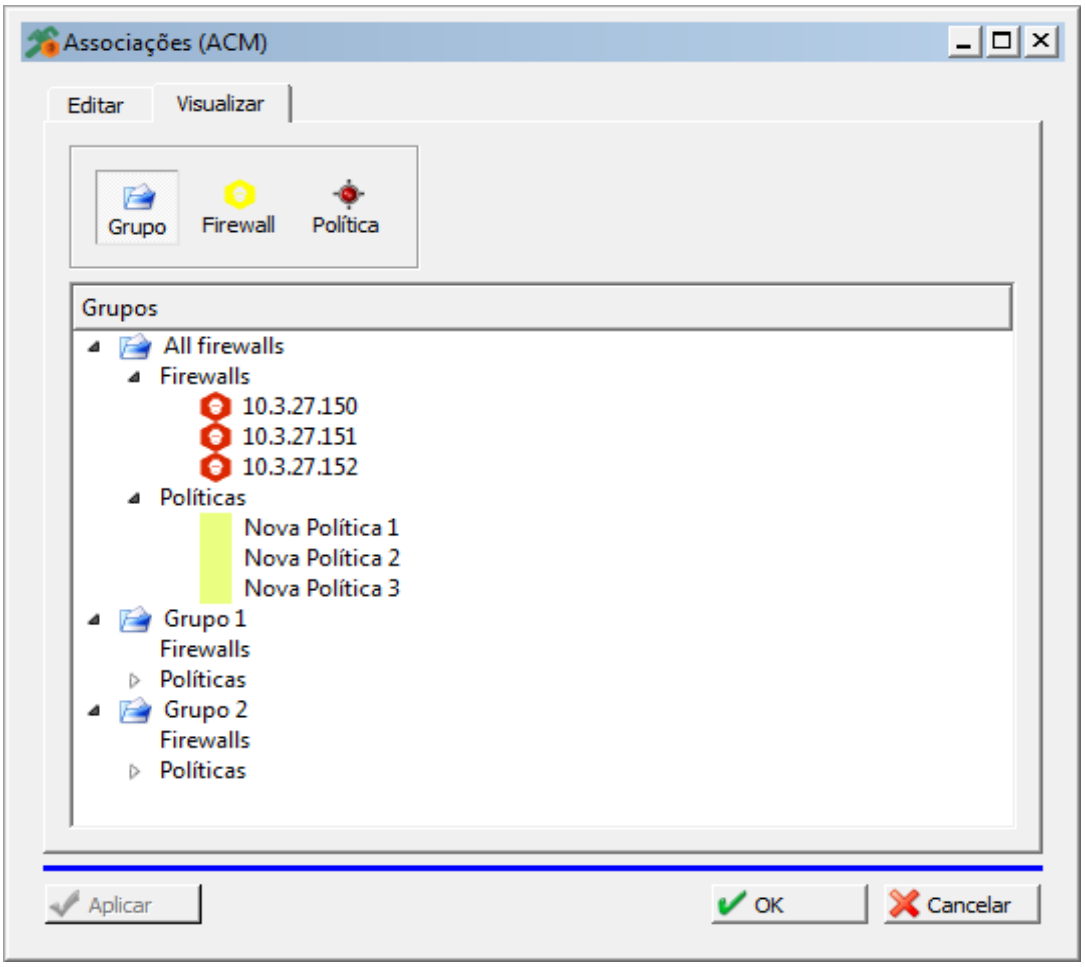

Figura 73 – Associações: Aba Visualizar

9.3 Exceções de validação de integridade

Para ter acesso a janela Exceções de validação de integridade deve-se:

Figura 74 – Exceções de validação de integridade

- Clicar no menu “*Políticas*”
- Selecione a opção “Exceções de validação de integridade”

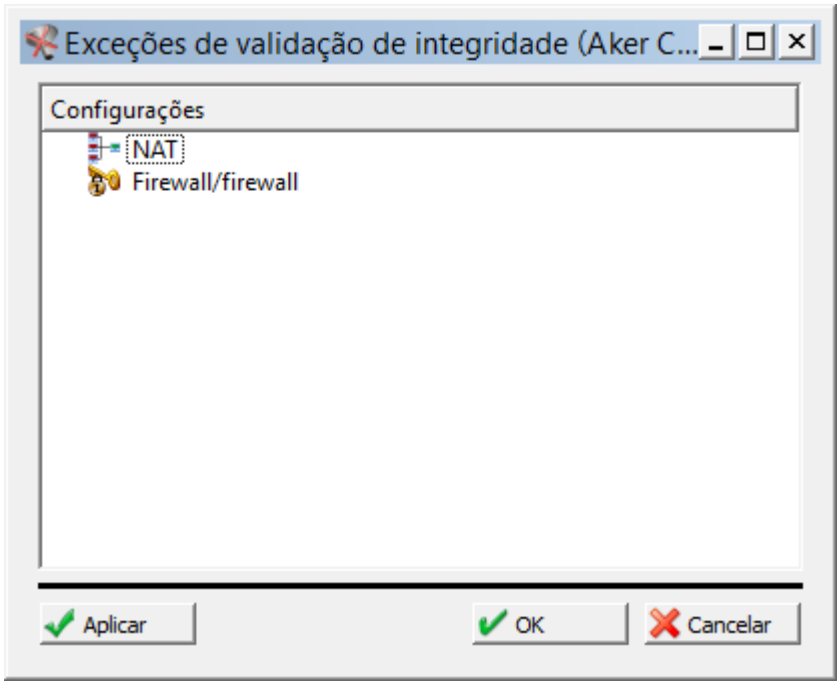

Figura 75 - Janela de configurações

Esta opção permite que o usuário crie exceções de validação na configuração do Aker Configuration Manager, possibilitando que Firewalls especificos possam ter suas configurações alteradas nos mesmos (*ou seja, efetuar alterações diretamente no Firewall, invés de efetuar estas alterações por meio do Aker Configuration Manager*).

Esta funcionalidade funciona apenas para Firewalls 6.7 patch 1 e posteriores, não sendo possível utilizar esta funcionalidade em versões obsoletas a estas descritas acima ou em Firewalls desatualizados.

Para que as alterações sejam feitas diretamente nos Firewalls, alem da criação das regras acima é necessario que o usuário desconecte o Firewall desejado do Aker Configuration Manager, caso contrario as alterações feitas não serão efetuadas. Para desconectar um Firewall do Aker Configuration Manager siga os passos a seguir:

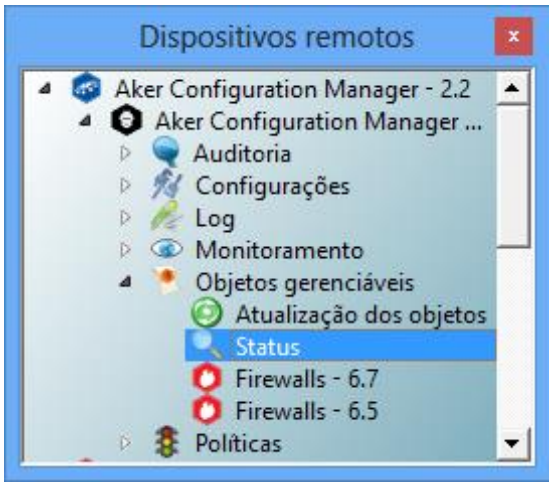

Figura 76 - Menu Status

- Clique no menu "*Objetos gerenciávies*"
- Selecione a opção "*Status*"

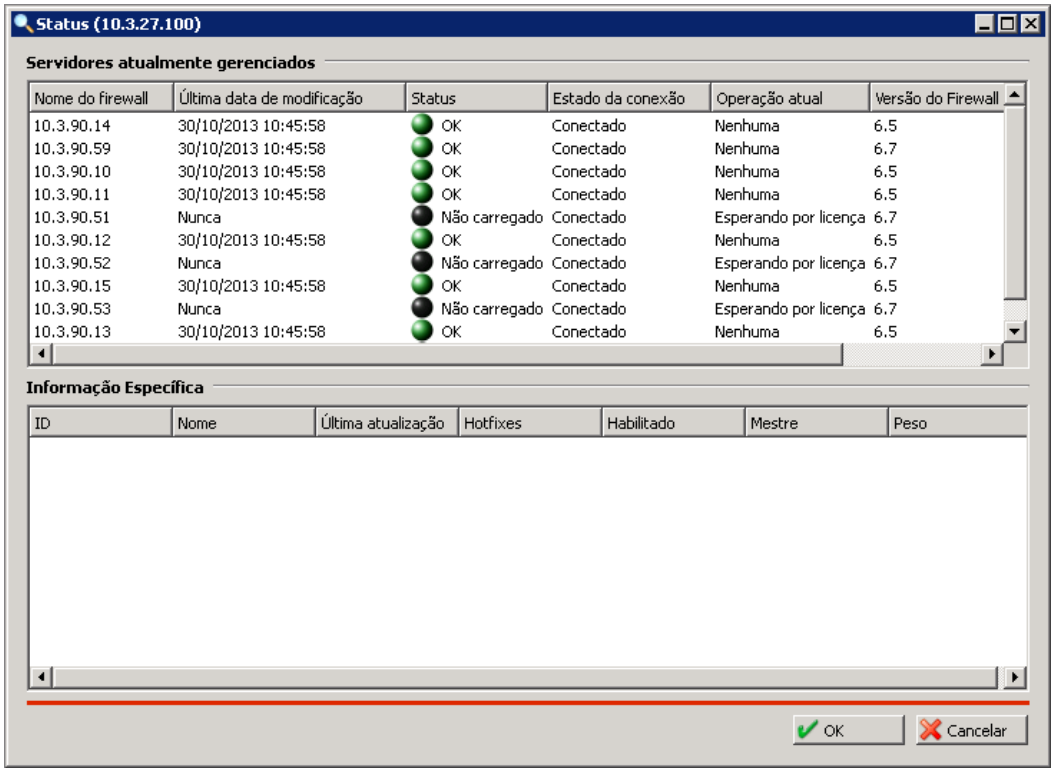
Status (10.3.27.100)
Servidores atualmente gerenciados
Nome do firewall | Última data de modificação | Status | Estado da conexão | Operação atual | Versão do Firewall
10.3.90.14 | 30/10/2013 10:45:58 | OK | Conectado | Nenhuma | 6.5
10.3.90.59 | 30/10/2013 10:45:58 | OK | Conectado | Nenhuma | 6.7
10.3.90.10 | 30/10/2013 10:45:58 | OK | Conectado | Nenhuma | 6.5
10.3.90.11 | 30/10/2013 10:45:58 | OK | Conectado | Nenhuma | 6.5
10.3.90.51 | Nunca | Não carregado | Conectado | Esperando por licença | 6.7
10.3.90.12 | 30/10/2013 10:45:58 | OK | Conectado | Nenhuma | 6.5
10.3.90.52 | Nunca | Não carregado | Conectado | Esperando por licença | 6.7
10.3.90.15 | 30/10/2013 10:45:58 | OK | Conectado | Nenhuma | 6.5
10.3.90.53 | Nunca | Não carregado | Conectado | Esperando por licença | 6.7
10.3.90.13 | 30/10/2013 10:45:58 | OK | Conectado | Nenhuma | 6.5
Informação Específica
ID | Nome | Última atualização | Hotfixes | Habilitado | Mestre | Peso
OK
Cancelar

Figura 77 - Janela Status

Esta janela permite visualizar os Firewalls que foram configurados e, que são gerenciados pelo Aker Configuration Manager. (Para mais informações veja o capítulo 10.3 Verificando Status)

Para desconectar um Firewall o usuário simplismente deve clicar com o botão direito sobre Firewall desejado e escolher a opção "Para operação". Ou clicar no botão localizado na parte superio da Control Center.

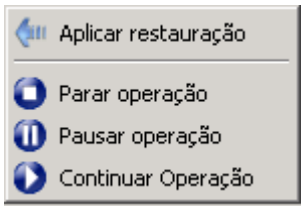

Figura 78 - Menu de opções da Janela Status

Figura 79 - Ícones de opção

Para mais informações sobre a janela *Status* veja o capítulo *10.3 Verificando Status*.

Ao se realizar quaisquer alterações de configuração no Configuration Manager ou em um dos Firewalls que ele gerencia, deve-se salvar essas alterações clicando no ícone "*Efetuar mudanças*" ( ) que é localizado na parte superior da Control Center, para que as modificações efetuadas sejam de fato salvas.

Visualizando o log do Sistema

10 Visualizando o log do Sistema

Neste capítulo mostraremos como visualizar os eventos do sistema, um recurso muito útil para acompanhar o funcionamento do Aker Configuration Manager e detectar possíveis ataques e erros de configuração.

O que são os eventos do sistema?

Eventos são as mensagens do firewall de nível mais alto, ou seja, não relacionadas diretamente a pacotes (como é o caso do log). Nos eventos, podem aparecer mensagens geradas por qualquer um dos três grandes módulos (filtro de pacotes, conversor de endereços e autenticação/criptografia) e por qualquer outro componente do firewall, como por exemplo, os proxies e os processos servidores encarregados de tarefas específicas.

Basicamente, o tipo de informação mostrada varia desde mensagens úteis para acompanhar o funcionamento do sistema (uma mensagem gerada todas as vezes que a máquina é reinicializada, todas as vezes que alguém estabelece uma sessão com o firewall, etc) até mensagens provocadas por erros de configuração ou de execução.

O que é um filtro de log?

Mesmo que o sistema tenha sido configurado para registrar todos os possíveis eventos, muitas vezes, o usuário está interessado em alguma informação específica (por exemplo, suponha que queira ver todas as mensagens do dia de ontem). O filtro de eventos é um mecanismo oferecido pelo Aker Configuration Manager para criar visões do conjunto total de mensagens, possibilitando que obtenha as informações desejadas facilmente.

O filtro só permite a visualização de informações que tiverem sido registradas nos eventos. Caso queira obter uma determinada informação deve-se inicialmente configurar o sistema para registrá-la e então utilizar um filtro para visualizá-la.

10.1 Configuração de log

Para ter acesso a janela de Configuração de log siga os passos a seguir:

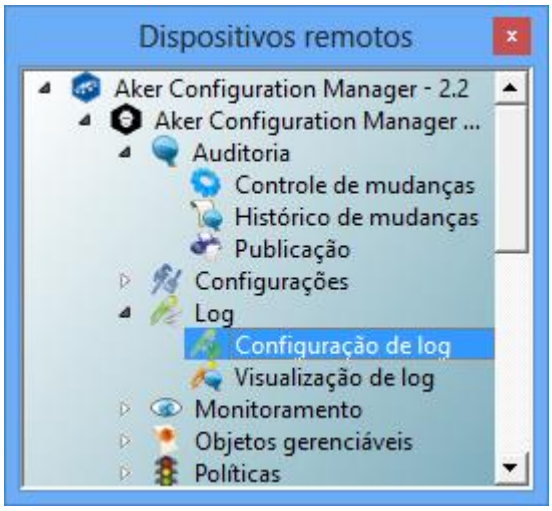

Figura 80 - Log: Configuração de log

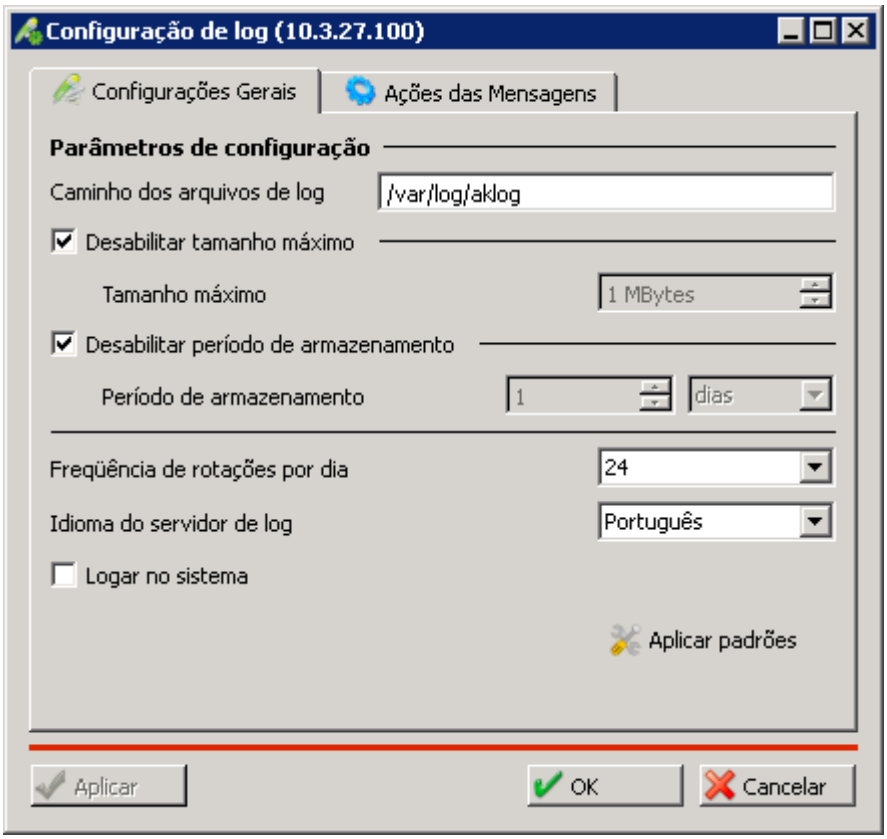

Figura 81 - Configurações Gerais

Parâmetros de configuração

- **Caminho dos arquivos de log:** Este campo informa o local que os logs serão salvos dentro do servidor.
- **Desabilitar tamanho máximo:** Desabilita ou habilita o tamanho máximo de logs que serão armazenados. Marcando esta opção todos os logs serão armazenados sem uma quantidade limite. Ao desmarcar a opção "*Desabilitar tamanho máximo"* serão armazendos apenas a quantidade de logs definida pelo usuario. Esta quantidade é definida em MB.
- **Desabilitar período de armazenamento:** Desabilita ou habilita o armazenamento de logs por periodo. Marcando esta opção todos os logs serão armazenados sem uma data limite. Ao desmarcar a opção "*Desabilitar período de armazenamento*" fará com que os logs sejam armazenados durante o periodo definido. Este periodo é definido em dias.
- **Frequencencias de rotação por dia:** Neste campo deve-se definir a quantidade de dias em que os logs ficaram salvos no servidor antes que estes sejam deletados.
- **Idioma do servior de log:** Neste campo deve-se definir qual o idioma que será usado no servidor de log. As opções disponíveis são: Português e Inglês.
- **Logar no sistema:** Ao selecionar esta opção o Aker Configuration Manager irá se conectar ao servidor via SYSLOG local.

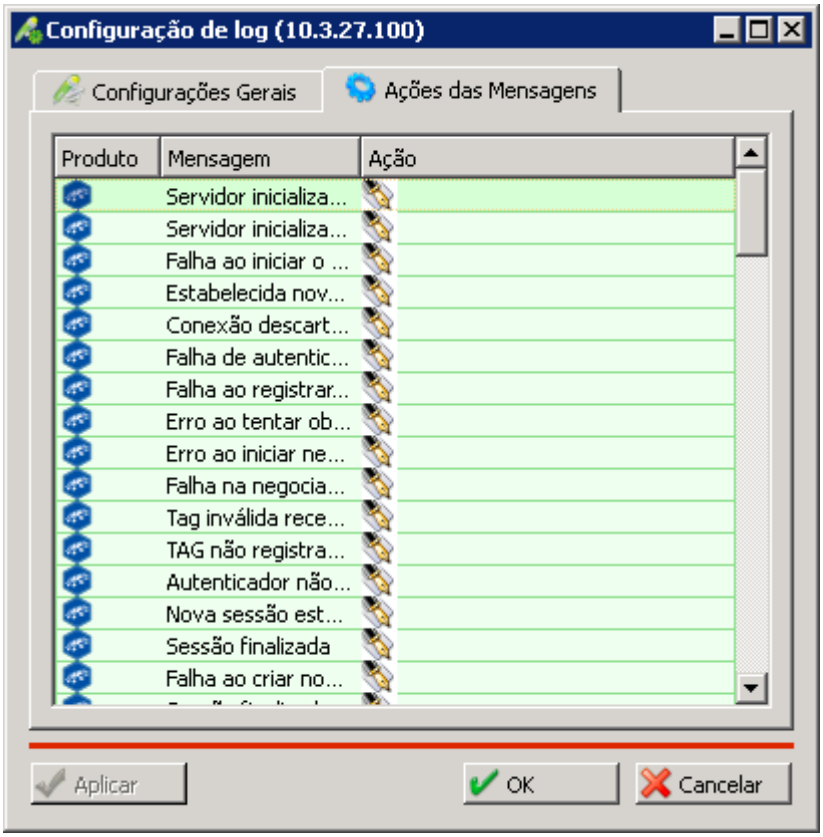

Figura 82 - Ações das Mensagens

Na aba Ações das mensagens o usuário pode selecionar quais mensagens serão logadas ou não. Para configurar uma mensagem especifica para logar, simplesmente clique com o botão direito sobre a mesma selecionando ou não a opção "Logar" ( ).

10.2 Visualização de log

Para ter acesso a janela de visualização do log siga os passos a seguir:

Figura 83 – Log: Visualização de log

- Clicar no menu *Configurações* que se deseja ver o log
- Selecionar a opção *Log*

A barra de ferramentas de Log

Todas as vezes que a opção *Log* for selecionada será mostrada automaticamente a barra de ferramentas de Log. Esta barra, que estará ao lado das outras barras, poderá ser arrastada e ficar flutuando acima das informações do Log. Ela tem o seguinte formato:

Figura 84 – Barra de ferramentas de Log

Significado dos Ícones:

- Abre a janela de filtragem do Aker Configuration Manager;

Figura 85 – Ícone: Abre a janela do Aker Configuration Manager

- Este ícone somente irá aparecer quando o Aker Configuration Manager estiver fazendo uma procura no Log. Ele permite interromper a busca do Configuration Manager;

Figura 86 – Ícone: Para a busca atual

- Exporta o log para diversos formatos de arquivos;

Figura 87 – Ícone: Exportar resultados

- Apaga o Log do Configuration Manager;

Figura 88 – Ícone: Limpar log

- Permite fazer uma atualização da tela de logs dentro de um determinado período definido no campo a seguir;

Figura 89 – Ícone: Habilita a atualização do log de acordo com o tempo especificado

- Define o tempo que o Configuration Manager irá atualizar a janela com informações de log;

Figura 90 – Ícone: Tempo para atualização das informações de log

- Percorre o Log para frente e para trás;

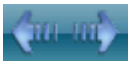

Figura 91 – Ícone: Mostrar resultados recentes e antigos

- Expande as mensagens de Log, mostrando as mesmas com o máximo de informação;

Figura 92 – Ícone: Expandir mensagens de log

- Ao clicar no ícone de filtro a janela abaixo irá aparecer:

A Janela de Filtro de Eventos

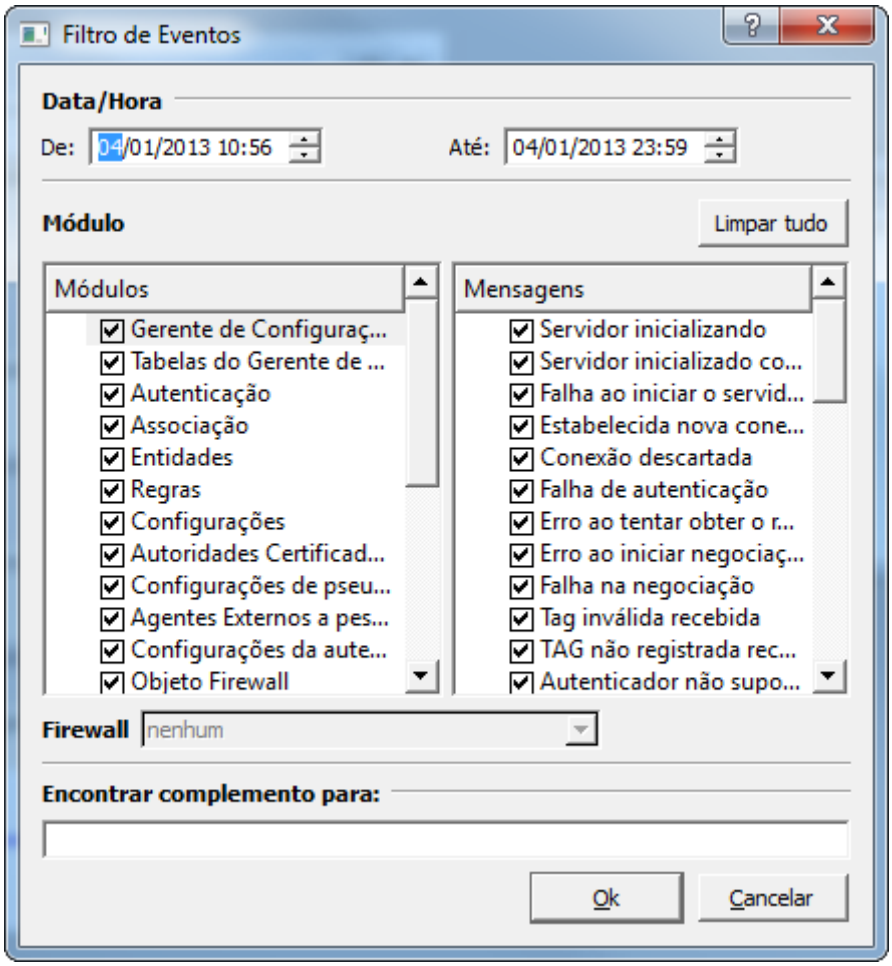

Figura 93 – Janela Filtro de eventos

O filtro padrão é configurado para mostrar todas as mensagens do dia atual. Para alterar a visualização para outros dias, pode-se configurar a **Data Inicial** e a **Data Final** para os dias desejados (a faixa de visualização compreende os registros da data inicial à data final, inclusive).

Além de especificar as datas, é possível também determinar quais mensagens devem ser mostradas. A opção **Filtrar por** permite escolher entre a listagem de mensagens ou de prioridades.

O campo **Firewall** permite selecionar o FW que se quer visualizar as configurações dos registros atuais dos logs.

Como última opção de filtragem, existe o campo **Encontrar complemento para**. Este campo permite que seja especificado um texto que deve existir nos complementos de todas as mensagens para que elas sejam mostradas. Desta forma, é possível, por exemplo, visualizar todas as páginas WWW acessadas por um determinado usuário, bastando para isso que coloque seu nome neste campo.

- O botão **OK** aplicará o filtro escolhido e mostrará a janela de eventos, com as informações selecionadas.
- O botão **Cancelar** fará com que a operação de filtragem seja cancelada e a janela de eventos será mostrada com as informações anteriores.

Janela de visualização de log

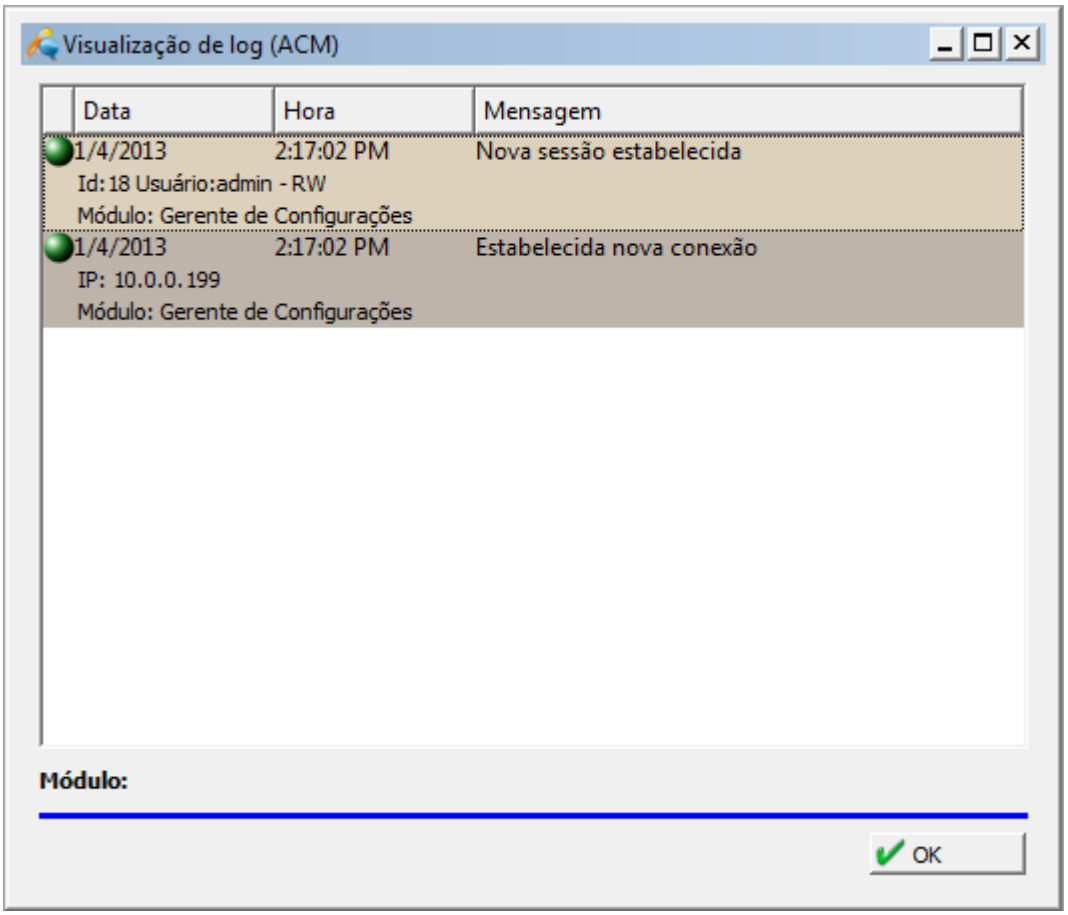

Figura 94 – Janela Log

A janela de eventos será mostrada após a aplicação de um filtro novo. Ela consiste de uma lista com várias mensagens. Normalmente, cada linha corresponde a uma mensagem distinta, porém existem mensagens que podem ocupar 2 ou 3 linhas.

Monitoramento

11 Monitoramento

Neste capítulo mostraremos como funciona o monitoramento dos firewalls que estão conectados ao Aker Configuration manager.

Para ter acesso as opções de monitoramento, clique no menu Monitoramento, no Configuration manager que desejar.

Figura 95 - Monitoramento

Janela de Alertas

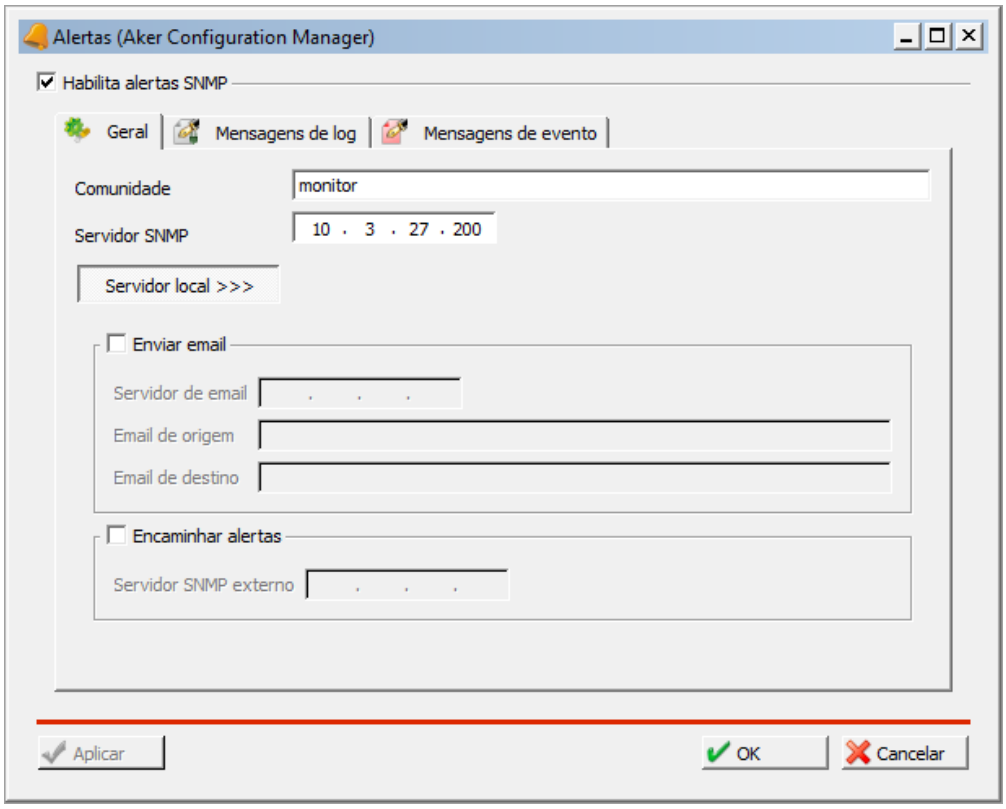

Figura 96 – Janela Alertas

Quando habilitada esta janela, enviará alertas dos serviços habilitados no Aker Configuration Manager via SNMP ou via email para o servidor.

Janela do Dashboard

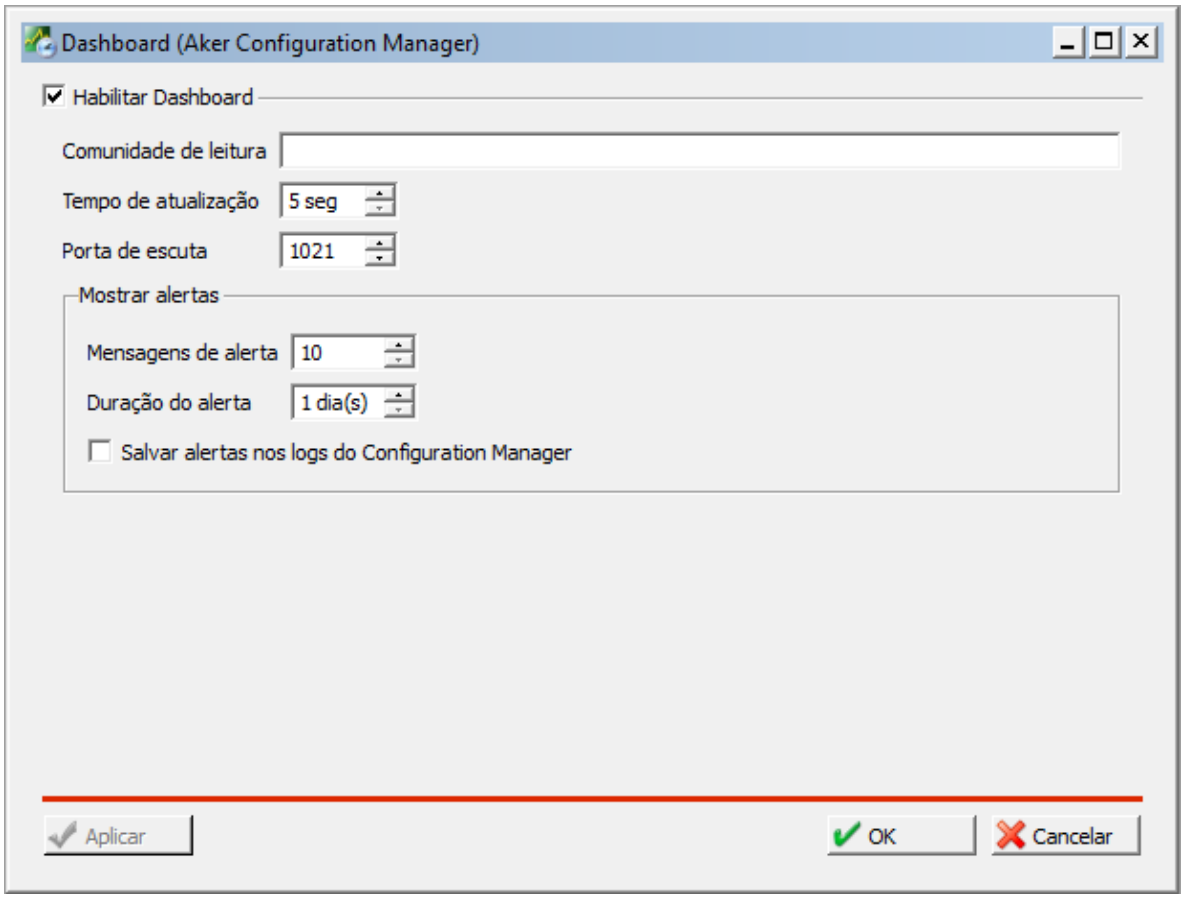

Figura 97 – Janela do Dashboard

Esta janela habilita a sincronização das informações dos firewalls gerenciados pelo Aker Configuration Manager com o servidor SNMP, o Aker Dashboard.

O download do Aker Dashboard pode ser feito no site: www.aker.com.br

11.1 Aker Dashboard

O Aker Dashboard é uma ferramenta que gerencia os firewalls que estão sendo gerenciados pelo Aker Configuration Manager, fornecendo acesso a informações importantes sobre o gerenciamento dos firewalls para o administrador da rede.

Para inserir um novo servidor clique no ícone ( ) e a janela abaixo será exibida:

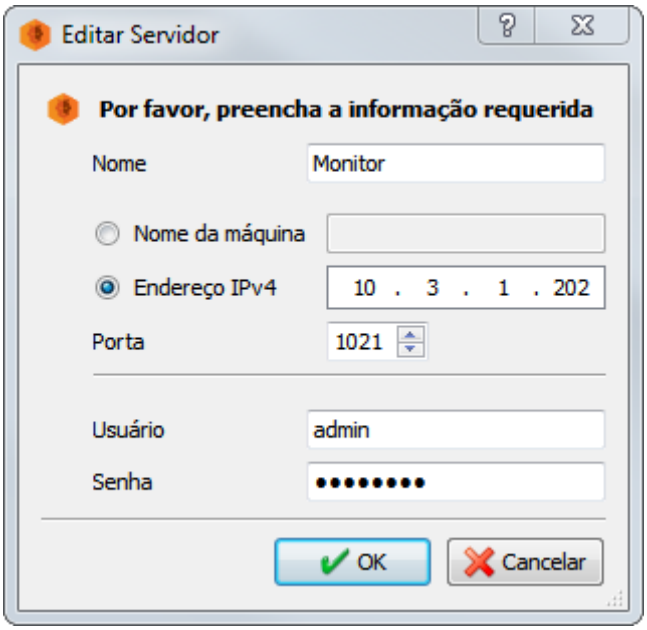

Figura 98 – Editando servidor no Aker Dashboard

Nome: Nome qual o servidor será referenciado.

Nome da máquina: Nome da máquina a qual o servidor irá se conectar.

Endereço IPv4: Endereço IP da máquina o qual o servidor irá se conectar.

Porta: Porta qual o servidor usará para se conectar à máquina.

Usuário: Nome de usuário da máquina que o servidor irá se conectar.

Senha: Senha do usuário da máquina que o servidor irá se conectar.

Ao definir as configurações do Dashboard, no Aker Configuration Manager, clique no botão ( ) para que estas novas configurações sejam efetuadas, e que a conexão com o Aker Dashboard seja efetuada com sucesso.

Na imagem a seguir, o Aker Dashboard informa ao administrador se o firewall 10.3.1.170 está ou não conectado, o *Uso de CPU, de Memória e de disco* do Firewall 150, facilitando assim a detecção e solução de problemas.

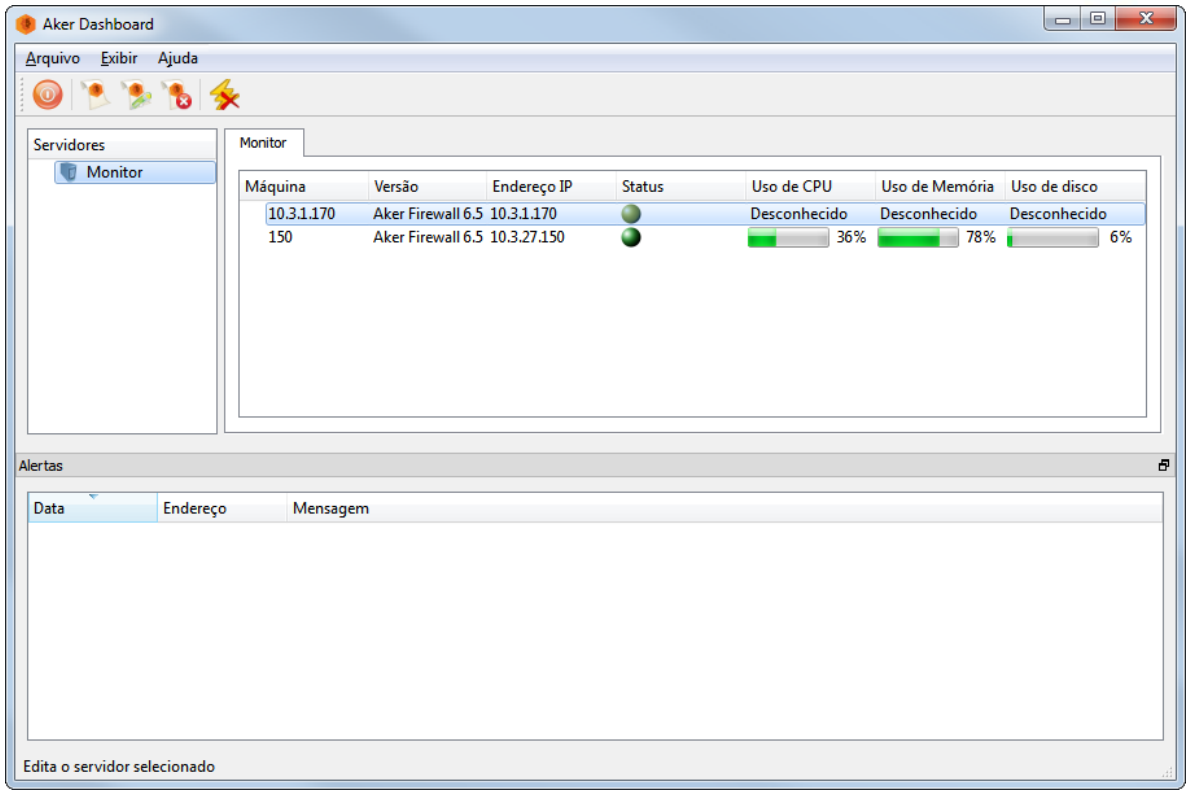

Figura 99 – Aker Dashboard

Gerenciando Firewalls

12 Gerenciando Firewalls

Neste capítulo mostraremos como se deve configurar os Firewalls que serão gerenciados pelo Configuration Manager.

Como configurar Firewalls no Configuration Manager?

Este produto permite que sejam gerenciados vários firewalls ao mesmo tempo, através da Interface Remota.

Cada Firewall pode ser acessado e configurado individualmente pelo Configuration Manager, e as informações de configuração são salvas em uma cópia local na máquina. Se outro usuário acessar o Firewall diretamente (ou seja, sem usar o Configuration Manager) e modificar sua configuração, na próxima vez que o Configuration Manager for utilizado, as modificações feitas diretamente serão perdidas. A cópia local feita pelo Configuration Manager será aplicada.

As configurações individuais que podem ser feitas são as mesmas disponibilizadas pela interface do Firewall.

Aker Firewall

Antes de configurar os Firewalls, para que aceitem as configurações do Configuration Manager, é necessário ativar as permissões de acesso através da janela "**Usuários Administrativos**" direto no Aker Firewall ao qual se deseja estabelecer uma conexão. Para realizar esse procedimento, deve-se:

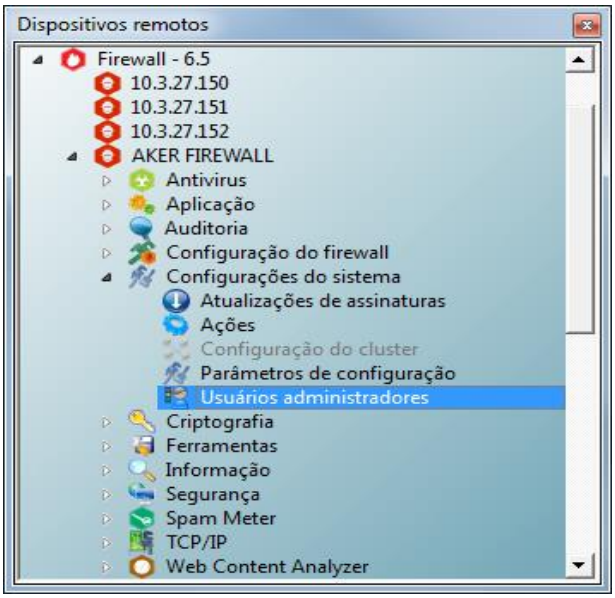

Figura 100 – Usuários administradores

- Clicar no menu *Configurações do Sistema* dentro de Firewall qual se deseja estabelecer a conexão
- Selecionar o item Usuários Administrativos

Aba Usuários Internos

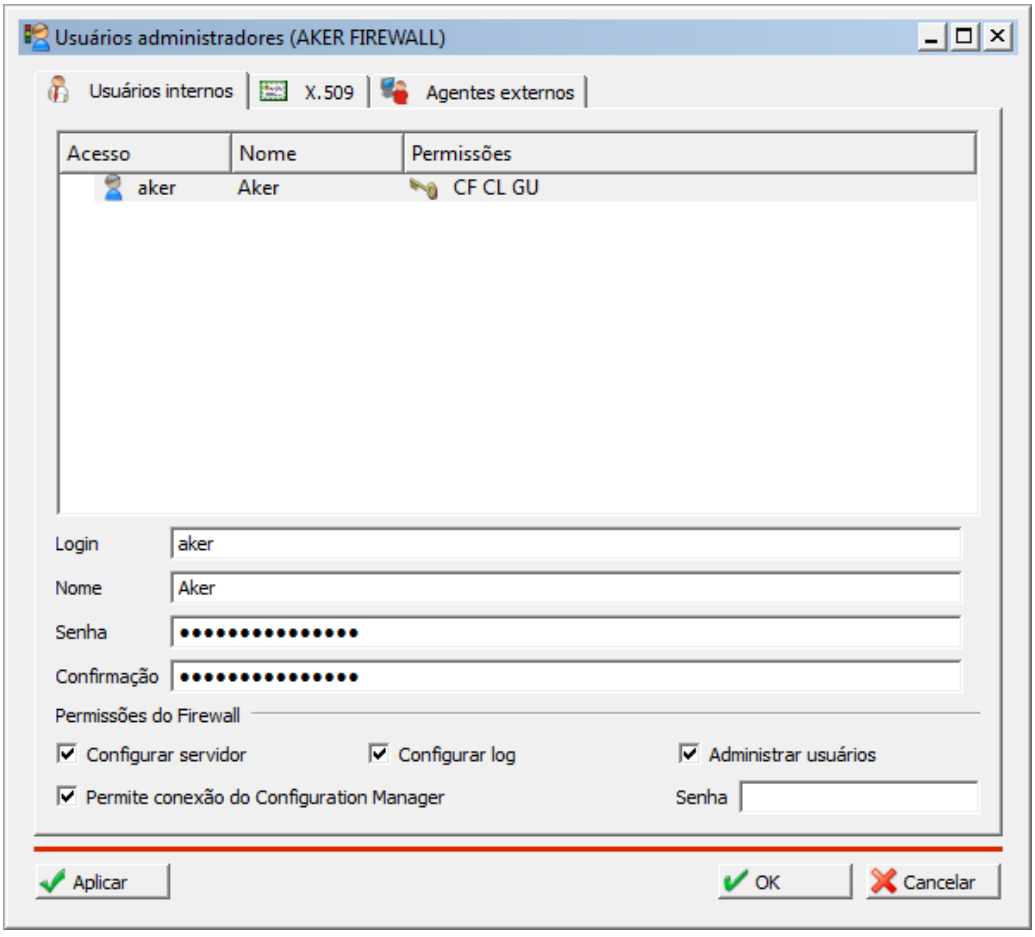

Figura 101 – Usuários Internos

Nesta aba, é necessário ativar a opção "**Permite conexão do Configuration Manager**" para que o Aker Configuration Manager consiga estabelecer com sucesso uma conexão com o Firewall, permitindo assim configurar os Firewalls através do Configuration Manager, do contrário o Firewall não permitirá essa conexão.

12.1 Configurando Firewalls no Aker Configuration Manager

Para criar um novo dispositivo remoto, deve-se:

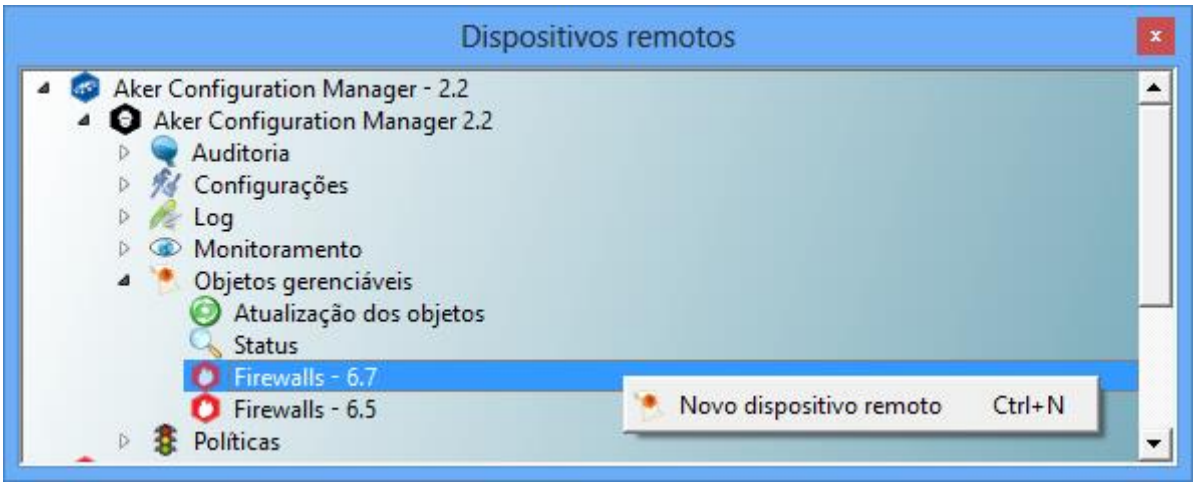

Figura 102 – Configurando um novo dispositivo remoto

- Clique no menu *Objetos gerenciáveis* dentro do Configuration Manager qual se deseja configurar
- Selecionar o item *Firewalls* do menu dispositivos remotos;
- Clique com o botão direito em Firewalls – 6.5 e Selecionar a opção ***Novo dispositivo remoto;***

Janela Editar Firewall

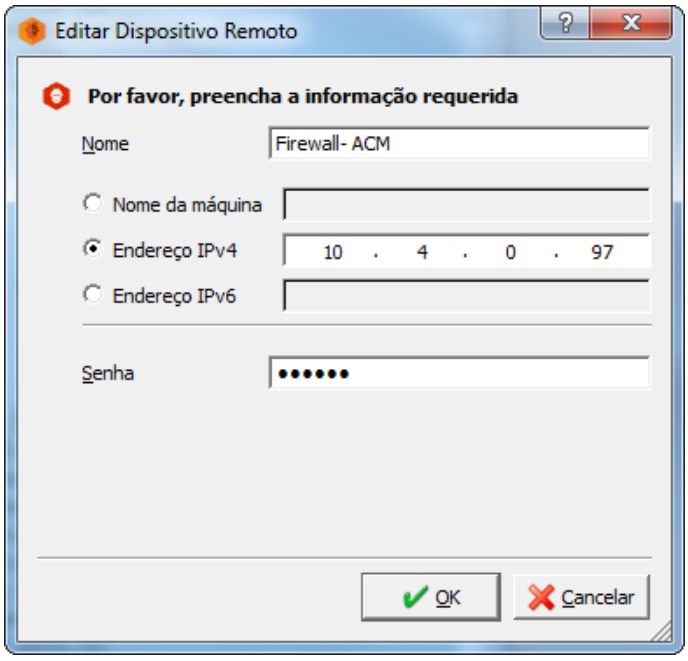

Figura 103 – Editando um novo dispositivo remoto

Esta janela permite editar os novos Firewalls que serão gerenciados pelo Aker Configuration Manager na Interface Remota. Mas, para realizar esta operação, antes é necessário selecionar uma opção, ou seja, marcar uma das três: nome da máquina, endereço IPv4 ou endereço IPv6.

O ícone localizado na parte superior dessa janela possibilita escolher o ícone e a cor desejada.

Nome: cadastrar o nome pelo qual o Firewall será referenciado na Interface Remota;

Nome da máquina: Ao selecionar está opção, deve-se indicar o nome de DNS da máquina do firewall;

Endereço IPv4: cadastrar o endereço IP versão 4 para conectar no Firewall;

Endereço IPv6: cadastrar o endereço IP versão 6 para conectar no Firewall;

Senha: a senha do usuário (a senha aparecerá na tela como vários asteriscos "*").

Esta senha deve ser a mesma cadastrada na aba "**Usuários internos**" da janela Usuários administrativos demonstrada no início deste capítulo. Caso contrário, o Firewall não aceitará a conexão pelo Aker Configuration Manager.

No final, basta clicar em **“Ok”** e o Firewall estará cadastrado com o tipo de configuração selecionada. No caso de cancelar o cadastro do Firewall, basta clicar em *Cancelar*.

12.2 Atualizando Objetos do Firewall

Para ter acesso a janela de *Atualização dos objetos*, deve-se:

Figura 104 – Atualizando objetos do Firewall

- Clicar no menu *Objetos gerenciáveis* do Aker Configuration Manager
- Selecionar o item Atualização dos objetos

Janela de Atualização dos Objetos

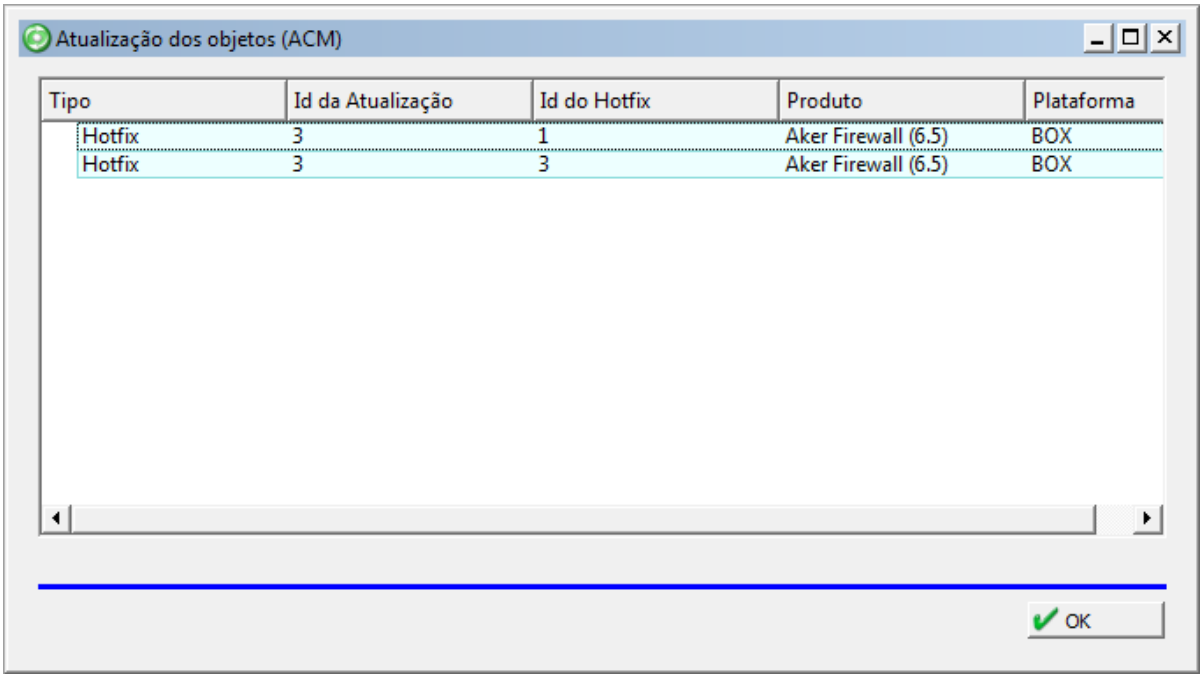

Figura 105 – Janela Atualização dos objetos

Esta janela possibilita que os Firewalls sejam atualizados, através de patches e/ou hotfixes com versões mais recentes disponíveis. É possível visualizar a versão aplicada, o patch que foi atualizado, a data e o tamanho do arquivo carregado. Existem duas maneiras para se carregar um arquivo de atualização de FW:

- Clicar no botão ( ) localizado na barra de ferramentas do Configuration Manager ou
- Clicar no ícone *Carregar* da janela Atualização dos objetos que se deseja configurar.

Assim que o arquivo for carregado, deve-se clicar no botão *Carregar patch* para que o patch de firewall seja enviado e salvo no CM.

Ver janela de status para explicações sobre como esse patch poderá ser aplicado nos firewalls.

O campo "**Descrição**" é apenas informativo, permite visualizar as correções presentes no patch e outras informações ao seu respeito.

12.3 Verificando Status

Para ter acesso a janela de Status, deve-se:

Figura 106 – Objetos gerenciáveis: Status

- Clicar no menu *Objetos gerenciáveis* da janela Dispositivos remotos do Aker Configuration Manager
- Selecionar o item *Status*

Janela Status

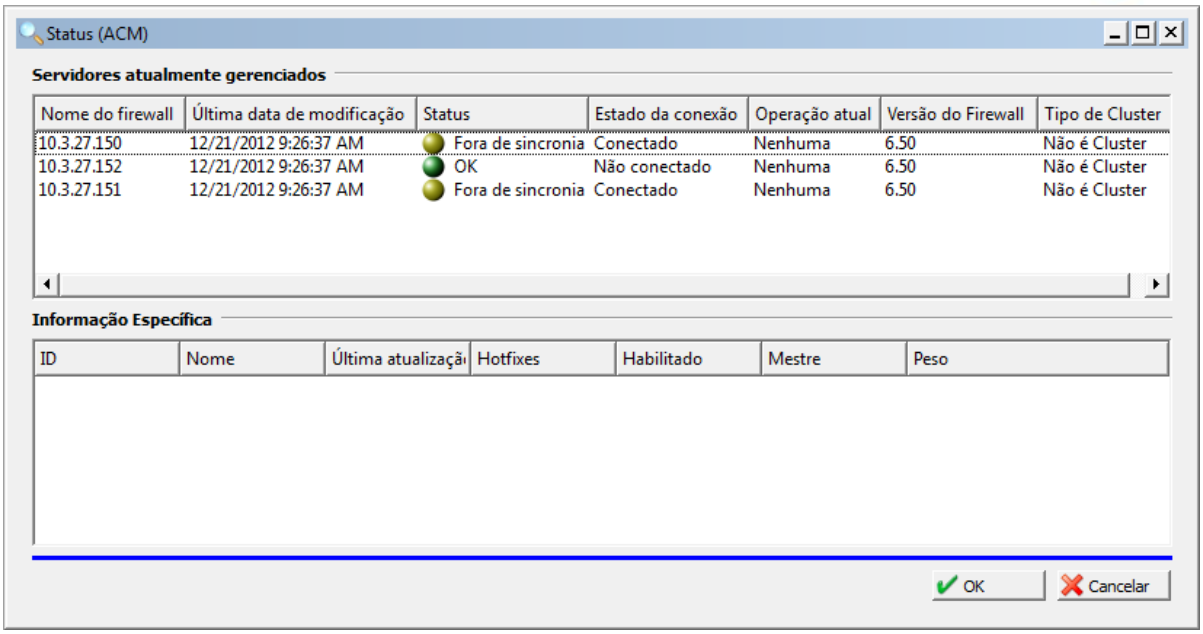

Figura 107 – Janela Status

Esta janela permite visualizar os Firewalls que foram configurados e, que serão gerenciados pelo Aker Configuration Manager.

Nome do Firewall: Este campo mostra o nome pelo qual o Firewall está sendo referenciado.

Última data de modificação: Data e hora que foi realizada a configuração.

Status: Define o status do Firewall que está sendo configurado.

- **Não carregado**: é quando o Aker Configuration Manager ainda não conseguiu ler a configuração completa do firewall.
- **Sujo**: é quando há modificações locais no Aker Configuration Manager que precisam ser aplicadas no firewall. Sempre que esse status aparecer na janela é uma indicação de que é necessário executar o comando "*Commit*", clicando no botão Efetuar mudanças. Quando as mudanças pendentes forem aplicadas corretamente, o status voltará para **"OK"**.

- **OK**: é quando o Aker CM está completamente sincronizado com o firewall. Não existe nenhuma modificação pendente a ser aplicada.
- **Desatualizado**: ocorre quando apenas uma parte da configuração foi aplicada no firewall. Ainda existem pendências.
- **Fora de sincronia**: é quando o Firewall foi modificado fora do contexto do Aker CM. Quando o Aker CM detecta essa situação, ele sobrescreve toda a configuração do firewall pela última que ele considera válida.

Estado da conexão: Define se o Firewall está conectado ou se conectando, ao Aker Configuration Manager.

Operação atual: Define a configuração realizada atualmente.

Versão do Firewall: Mostra a versão do Firewall que foi configurado.

Tipo de Cluster: Mostra o tipo de cluster dos firewalls.

Firewalls em cluster também podem ser gerenciados pelo ACM.

Ao clicar com o botão esquerdo sobre um dos Firewalls gerenciados pelo Aker Configuration Manager na janela de Status, será permitido escolher uma das opções disponíveis conforme demonstrado na janela a seguir:

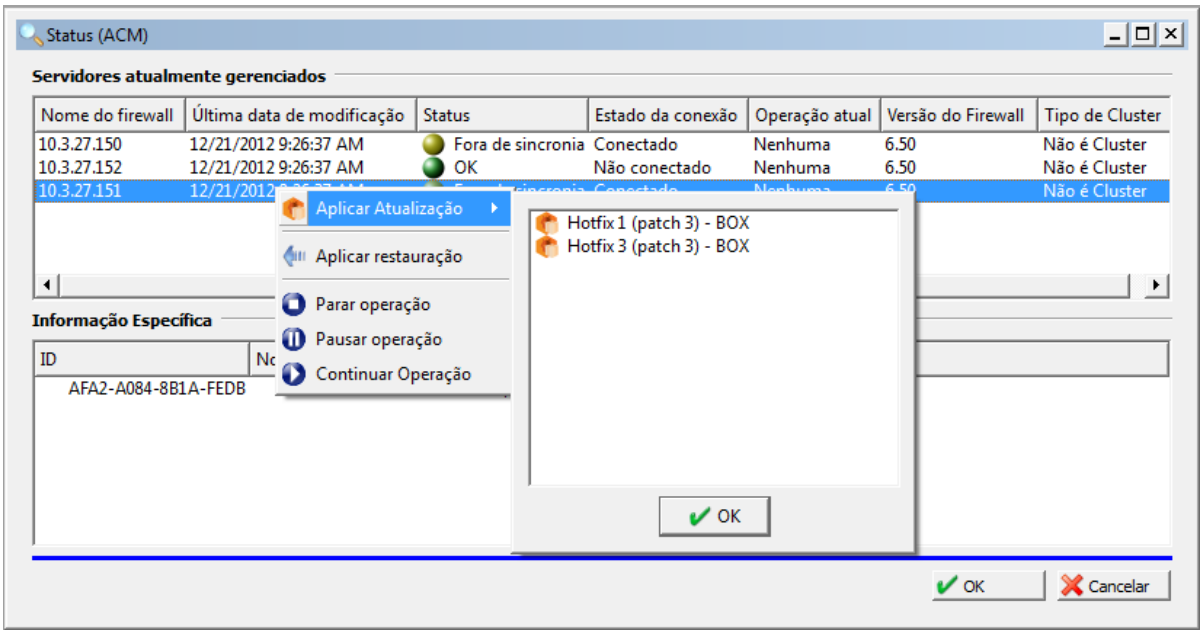

Figura 108 – Menu de opções da Janela de Status

Aplicar Atualização: Esta opção permite aplicar nos Firewalls selecionados o patch ou hotfix previamente carregado na janela "Atualização dos Objetos", mostrada anteriormente.

Parar operação: Permite encerrar a conexão do Configuration Manager com os Firewalls selecionados e interromper qualquer operação (ver coluna "**Operação atual**") que estiver sendo realizada.

Pausar operação: Permite pausar a operação que estiver sendo exibida na coluna "**Operação atual**" até que a opção *Continuar* seja acionada.

Continuar operação: Esta opção permite estabelecer nova conexão do Configuration Manager com os Firewalls selecionados e continuar qualquer operação que estava pendente previamente.

A barra de Ferramenta de Status

Todas as vezes que a janela Status for aberta, será mostrada automaticamente a barra de ferramentas de Status localizada na parte superior do Control Center ao lado das outras barras. Ela tem o seguinte formato:

Figura 109 – Barra de ferramentas de Status

Permite fazer atualizações da tela de Status e esse período de atualização ocorre de tempos em tempos de acordo com o configurado no campo a seguir.

Define o tempo que o Configuration Manager irá atualizar as informações da janela de Status.

Os demais botões (Parar, Pausar e Continuar Operação) já foram apresentados anteriormente.

Aker Configuration Manager

Apêndice B – Copyrights e Disclaimers

13 Apêndice A - Copyrights e Disclaimers

Neste apêndice estão listados os disclaimers das bibliotecas e códigos fontes de terceiro utilizados no Aker Configuration Manager. Estes disclaimers se aplicam apenas às partes explicitamente citadas e não ao Aker Configuration Manager como um todo. Eles estão citados aqui devido a exigências das entidades desenvolvedoras:

Biblioteca DES

Copyright (C) 1995 Eric Young (eay@mincom.oz.au)
All rights reserved.

This library and applications are
FREE FOR COMMERCIAL AND NON-COMMERCIAL USE
as long as the following conditions are aheared to.

Copyright remains Eric Young's, and as such any Copyright notices in
the code are not to be removed. If this code is used in a product,
Eric Young should be given attribution as the author of the parts used.
This can be in the form of a textual message at program startup or
in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
must display the following acknowledgement:
This product includes software developed by Eric Young (eay@mincom.oz.au)

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED
TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA,
OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.

The licence and distribution terms for any publically available version or
derivative of this code cannot be changed. i.e. this code cannot simply be
copied and put under another distribution licence
[including the GNU Public Licence.]

Biblioteca de criptografia libcrypto

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
All rights reserved.

This package is an SSL implementation written
by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as
the following conditions are aheared to. The following conditions
apply to all code found in this distribution, be it the RC4, RSA,
lhash, DES, etc., code; not just the SSL code. The SSL documentation
included with this distribution is covered by the same copyright terms
except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in
the code are not to be removed.
If this package is used in a product, Eric Young should be given attribution

as the author of the parts of the library used.
This can be in the form of a textual message at program startup or
in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
must display the following acknowledgement:
"This product includes cryptographic software written by
Eric Young (eay@cryptsoft.com)"
The word 'cryptographic' can be left out if the rouines from the library
being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from
the apps directory (application code) you must include an acknowledgement:
"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The licence and distribution terms for any publically available version or
derivative of this code cannot be changed. i.e. this code cannot simply be
copied and put under another distribution licence
[including the GNU Public Licence.]

Biblioteca SNMP

Copyright 1997 by Carnegie Mellon University

All Rights Reserved

Permission to use, copy, modify, and distribute this software and its

documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Códigos do FreeBSD

Copyright (c) 1982, 1986, 1993
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions
and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following
acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or
promote products derived from this software without specific prior written permission.

This software is provided by the regents and contributors ``as is"
and any express or implied warranties, including, but not limited
to, the implied warranties of merchantability and fitness for a
particular purpose are disclaimed. In no event shall the regents or
contributors be liable for any direct, indirect, incidental, special,
exemplary, or consequential damages (including, but not limited
to, procurement of substitute goods or services; loss of use, data,
or profits; or business interruption) however caused and on any
theory of liability, whether in contract, strict liability, or tort
(including negligence or otherwise) arising in any way out of the
use of this software, even if advised of the possibility of such
damage.

Algoritmo MD5

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data
Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified
as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this
software or the suitability of this software for any particular purpose. It is provided "as is" without

express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

Agente SNMP

Copyright (c) 1996, 1997 Wes Hardaker and the University of California at Davis

COPYRIGHT

Many portions of the code in this package were distributed by Carnegie Mellon University. All other code and changes to the original code written by Wes Hardaker at the University of California at Davis is copyrighted under the following copyright:

Permission is granted to use, copy, modify, and distribute this software and documentation. This
software is distributed freely and usage of it is not subject to fees of any kind. It may be included in
a software compact disk set provided that the author is contacted and made aware of its distribution.

Biblioteca de números extendidos LInteger

LInteger Version 0.2 Source Code and Documentation

Copyright (C) 1996 by Leonard Janke

This source code and documentation may be used without charge for both commercial and non-commercial use. Modification of the source code or documentation is allowed provided any derivate work is clearly indentified as such and all copyright notices are retained unmodified. Redistribution of the source code or documentation is unlimited, except by the limits already mentioned, provided that the redistribution is not for profit. Those wishing to redistribute this source code or documentation or any work derived from either for profit must contact Leonard Janke (janke@unixg.ubc.ca) to work out an acceptable arrangement.

Anyone who wishes to distribute a program statically linked against the functions provided may do so providing that he or she include a copy of this note with the program.

Distribution of libraries compiled from this source code is unlimited if the distribution is not for profit and this copyright notice is included. Those wishing to distribute libraries compiled from this source code or any work derived from it for profit must contact Leonard Janke (janke@unixg.ubc.ca) to work out an acceptable arrangement.

Anyone using this source code or documentation or any work derived from it, including, but not limited to, libraries and statically linked executable, must do so at his or her own risk, and with understanding that Leonard Janke will not be held responsible for any damages or losses that may result.